Teil 2

Lotus Domino: Administration

I

Das Domino-System

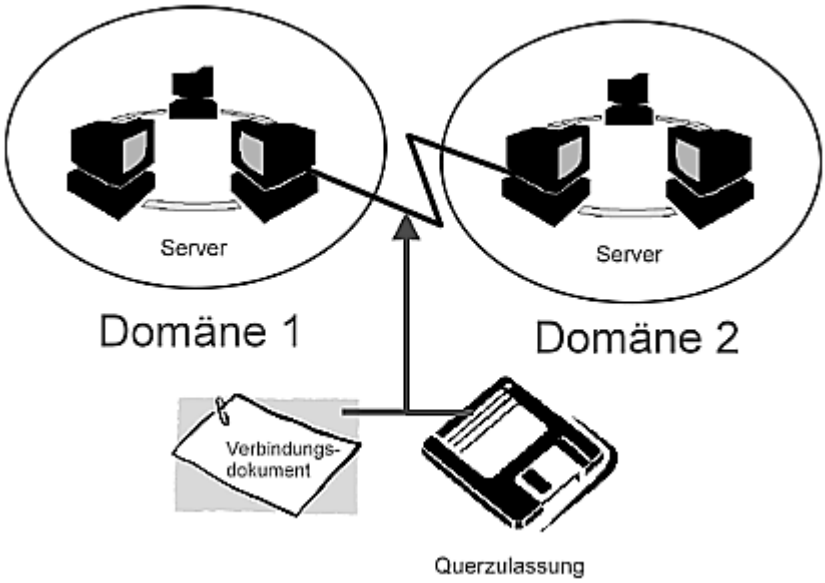
Aus einer einfachen Anwendung zur Verwaltung von Informationen hat sich Lotus Notes zu einem System von Programmen und darauf basierenden Anwendungen entwickelt. Der Server-Bereich mit dem Namen Lotus Domino und die verschiedenen Clients (Notes, Administrator und Designer) sind auf unterschiedlichen Hardwareplattformen und Betriebssystemen verfügbar. Die Verwaltung und Steuerung eines solchen Systems wird um so aufwendiger, je mehr Geräte, Netzwerke, Benutzer und Anwendungen darin

zu finden sind. Als zentrales Steuerungsinstrument kann der Administrator-Client eingesetzt werden. Mit seiner Hilfe werden viele unterschiedliche Elemente des Domino-Systems überwacht und bearbeitet.

1.1 Elemente

Zunächst einmal besteht das Domino-System aus Servern und den dazugehörigen Clients. Die Software ist jeweils auf einer Hardware-Plattform und dem dazugehörigen Betriebssystem installiert. Verbunden ist das Ganze dann durch ein oder mehrere Netzwerke. Damit eine Verwaltung der Geräte und ihrer Benutzer möglich wird, kennt Lotus Domino Verzeichnisse, die wiederum gruppiert werden können.

Eine Gruppe von Servern, Clients und Benutzern, die über ein oder mehrere Netzwerke miteinander verbunden sind und die ein Verzeichnis besitzt, wird als Domäne bezeichnet.



Domino-Domänen

Bei der Installation ermittelt das System den ersten Server der Domäne und installiert dort das Domänen-Verzeichnis (früher: Namens- und Adressbuch). In diesem Verzeichnis werden Personen, Gruppen, Server und weitere Informationen in Form von Dokumenten verwaltet. Die verschiedenen Server-Prozesse verwenden diese Dokumente für ihre Arbeit.

In den Server-Dokumenten werden auch die Netzwerke der Domäne verwaltet. Dabei ist unter einem Netzwerk die technische Verbindung von Rechnern über ein einheitliches Protokoll zu verstehen.

Die Adressverzeichnisse dienen als Informationsquelle beim Anlegen, Versenden und Weiterleiten von e-Mails. Gleichzeitig werden sie im Rahmen des Sicherheitskonzeptes von Lotus Domino eingesetzt.

Für die Verwaltung eines Domino-Systems werden eine ganze Reihe von Datenbanken (z.B. Log.nsf) dazu verwendet, Vorgänge aufzuzeichnen und in Form von Berichtsdokumenten und Ansichten wiederzugeben. Damit können viele Problemursachen erkannt und bereinigt werden.

Ein weiteres Steuerungselement stellt die Datei „notes.ini“ dar. Im Verzeichnis „Domino“ für die Server und „Notes“ für die Clients wird diese Datei als Textdatei gespeichert und enthält eine ganze Reihe von Einträgen, die den Ablauf von Programmen steuern.

Der Administrator-Client stellt eine grafische Oberfläche zur Verfügung, über die alle Elemente des Domino-Systems verwaltet werden können.

1.2 Die Aufgaben des Systemadministrators

Ein Domino-System, wenn es seine Aufgaben erfüllen soll, muss genau geplant sein. Die Aufgaben des Systemadministrators beginnen deshalb bereits in der Planungsphase des Systems. Bevor Hard- oder Software angeschafft und installiert werden können, sind die Anforderungen zu definieren, denen das System genügen soll. Dabei stellen sich die unterschiedlichsten Fragen:

- Wie viele Benutzer sollen das System nutzen?
- Werden neben der e-Mail-Funktion andere Anwendungen eingesetzt und wer wird damit arbeiten?
- Welche Hardware ist bereits installiert?
- Welches System-Know-how ist vorhanden?
- Müssen unterschiedliche Hardware-Plattformen eingesetzt werden?
- Sind mehrere Standorte einzubeziehen?
- Welche Netzwerk- und DFÜ-Systeme werden benötigt?
- Sollen Web-Funktionen einbezogen werden?

Sicher wird man in der Regel vom bestehenden EDV-System ausgehen und alle erforderlichen Erweiterungen und Änderungen definieren. Soll die Installation und Verwaltung des Domino-Systems im Hause durchgeführt werden, so sind der Schulungsaufwand und die entsprechende Einarbeitungszeit zu berücksichtigen.

Sind die planungstechnischen Vorbereitungen abgeschlossen, kann mit der Installation und Integration der erforderlichen Hardware

begonnen werden. Die Hardware-Ressourcen sind anhand der Anwendungen zu testen, die auf der Basis von Lotus Domino eingesetzt werden sollen. Das Domino-System stellt oft hohe Anforderungen an die Ausstattung von Servern und Clients. Auch die Netzwerkbelastung kann sich stark verändern durch den Einsatz von Domino. Sind Außenstellen in das System einzubinden, muss die Remote-Konfiguration installiert und getestet werden.

Erst, wenn die Hardware zumindest in einer Basisinstallation verfügbar ist, kann mit der Installation der Server- und Client-Software begonnen werden. Im nächsten Schritt sind die Systemkonfiguration und die Benutzerregistrierung durchzuführen. Damit ein brauchbares und zukunftsfähiges Namenssystem entsteht, ist ein Plan der Unternehmensorganisation und eine Umsetzung in die Domino-Namenshierarchie erforderlich.

Nach Installation der Client-Arbeitsplätze und der Einrichtung von Replikation und Mail-Routing können spezielle Anwendungen implementiert werden.

Ist das ganze System eingerichtet, hat der Systemadministrator die Aufgabe, das System zu optimieren und die erforderlichen Änderungen durchzuführen. Dazu steht ihm der Administrator-Client zur Verfügung, eine Anwendung, in der viele Werkzeuge zur Überwachung und Steuerung des Domino-Systems enthalten sind.

2

Der Administrator-Client

Bei dem Administrator-Client handelt es sich um ein eigenständiges Programm, das getrennt installiert werden muss. Er ist das wichtigste Werkzeug des Systemadministrators. Es gibt verschiedene Wege, wie der Administrator-Client gestartet werden kann:

- über ein Symbol auf dem Desktop
- mit Hilfe des Start-Menüs

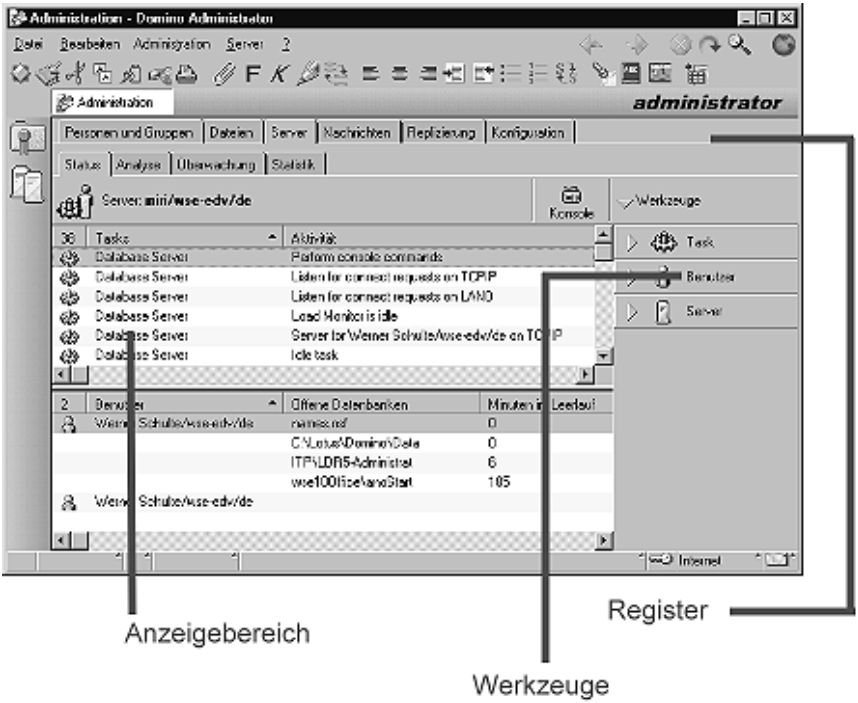
- durch Anklicken des Lesezeichens im Notes-Client
- durch Verwendung des Menüs „Datei / Extras / Server-Administration“

Startmenü für den Administrator-Client

2.1 Das Aussehen des Clients

Jeder, der einmal mit der spartanischen Oberfläche der Server-Konsole gearbeitet hat, wird bei der Administration mit Hilfe dieses Programmes eine echte Überraschung erleben: die grafische Oberfläche vermittelt ein übersichtliches Bild über die Verwaltungsfunktionen des Domino-Systems. Über die Einteilung in Bereiche und Register kann schnell und einfach zu den einzelnen Übersichten und Dokumenten gewechselt werden.

Es sind zunächst zwei große Bereiche zu erkennen: die Funktionsauswahl mit ihrer Registerstruktur (Personen und Gruppen, Dateien, Server, Nachrichten, Replizierung und Konfiguration) und der Fensterbereich zur Bearbeitung der Funktionen und Objekte.



Der Administrator-Client

2.1.1 Die Bereichsregister

Lotus hat die Aufgaben des Administrator-Clients in Bereichen zusammengefasst, die über Register einer Tabelle ausgewählt werden.

Bereichsregister

Die Register bieten Arbeitsbereiche für:

- Personen und Gruppen

  Es wird eine Auswahl der Ansichten des Domino-Verzeichnisses der Domäne angeboten (Personen, Gruppen, Mail-In-Datenbanken, Konfigurationsprofile und Zertifikate. In der Werkzeugleiste werden Hilfsmittel für die Verwaltung von Personen und Gruppen angeboten.

- Dateien

  Übersicht der Dateien des ausgewählten Servers. In der Werkzeugleiste stehen die passenden Tools (Komprimieren, Index, Replikation etc.) zur Verfügung.

- Server

  Überwachung des Server-Status, Analyse-Werkzeuge und Statistiken.

- Nachrichten

  Informationen zu den Mail-Benutzern sowie zu den e-Mails, die noch nicht ausgeliefert sind.

- Replizierung

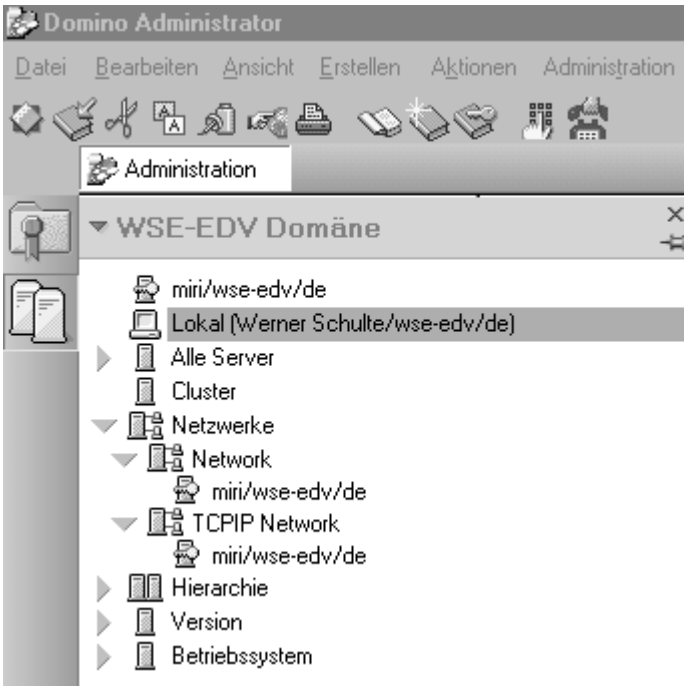
  Replikationsereignisse und die Topologie der Replikation

- Konfiguration

  Verwaltung wichtiger Abschnitte in Server-Dokumenten.

2.1.2 Lesezeichenseiten mit Servern

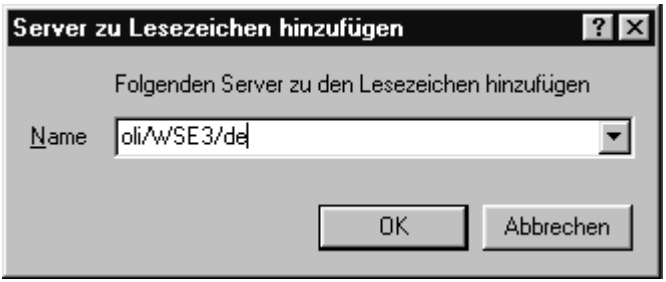
In Abhängigkeit von den Registern werden im unteren Bereich die dazugehörigen Fenster geöffnet. Ganz links in der Lesezeichenseite wird zunächst festgelegt, welcher Server oder welche Domäne verwendet werden soll. Der Einstieg über andere Hierarchien wie z. B. über das Netzwerk erleichtert das Auffinden von Servern.



Lesezeichenseite und Objektauswahl

Aus den globalen Informationen über die verwalteten Domänen und Server wird eine Struktur erzeugt, wie sie z.B. vom Explorer her bekannt ist. Die Lesezeichenseite mit den Servern kann fest am linken Rand positioniert werden. Bei der Standardeinstellung verschwindet sie, sobald der Cursor im rechten Fenster positioniert wird.

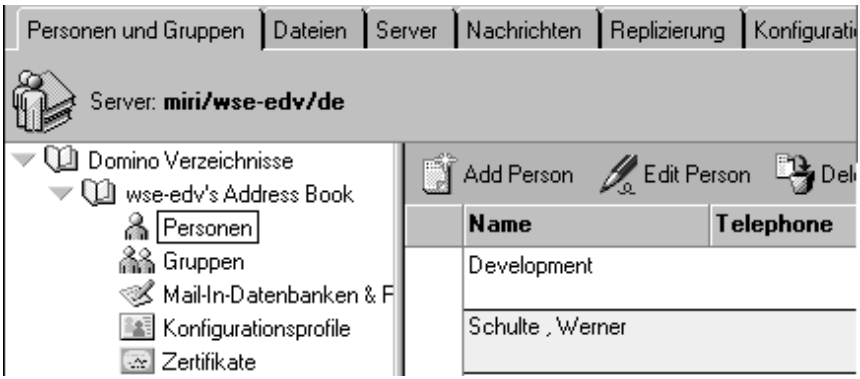
In der Lesezeichenseite des Ordners „Favoriten“ können eigene Server-Zusammenstellungen abgelegt werden. Das erfolgt über das Menü „Administration / Server zu Lesezeichen hinzufügen“.



Server zu Lesezeichen hinzufügen

2.1.3 Der Anzeigebereich für Einzelobjekte

Weiter rechts befindet sich das Fenster für die Auswahl von Einzelobjekten, die zu den jeweiligen Funktionen gehören. Beim Starten des Administrator-Clients wird standardmäßig das Register zur Verwaltung von Personen und Gruppen geöffnet.



Fenster mit Personen und Gruppen

Je nach Auswahl der Register ändern sich die darunter angezeigten Fenster. Über die Icons im Einzelauswahlfenster ruft man die dazugehörigen Ansichten des Domino-Verzeichnisses auf. Dort werden, wie üblich, die einzelnen Dokumente der Personen oder Gruppen aufgelistet und können mit Doppelklick bearbeitet werden.

An diesem Beispiel läßt sich sehr schön das Prinzip des Administrator-Clients verdeutlichen. Bis zur Ebene des Einzelauswahlfensters wirkt die Oberfläche des Clients. Im Rahmen der Personen-

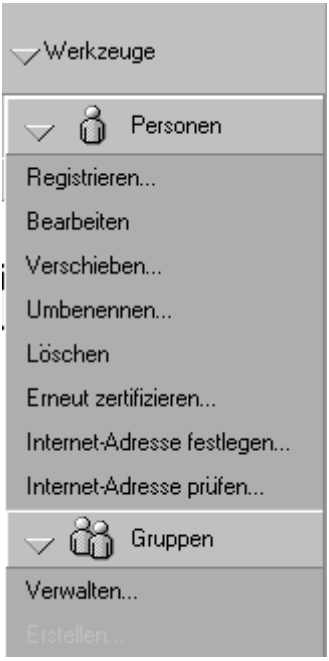
auflistung wird die Ansicht „Kontakte“ des Domino-Verzeichnisses angezeigt und die Bearbeitung der Daten erfolgt direkt im Domino-Verzeichnis.

Personendokument

Da die angezeigten Werte zum Teil aktuell aus den Ursprungsdokumenten ermittelt werden, kann es etwas Zeit in Anspruch nehmen, bis die Werte im Fenster erscheinen.

2.1.4 Die Werkzeugleiste

Am rechten Rand befindet sich die Werkzeugleiste. In ihr sind Aktionen aufgeführt, die mit dem jeweiligen Objekt durchgeführt werden können.



Werkzeuge

Die Werkzeuge greifen auf unterschiedliche Datenbanken und Dokumente zu. Der Administrator muss nicht wissen, wo die Informationen gespeichert werden, sondern kann die Verwaltung aus dem Kontext heraus vornehmen.

Diese Seite ist zur Zeit nicht belegt.

2.2 Mit dem Administrator-Client arbeiten

Im Administrator-Client sind wichtige Funktionen zusammengefasst, die einzeln in unterschiedlichen Datenbanken und Dateien ihre Auswirkung finden. Die wichtigste Sammlung findet sich im Domino-Verzeichnis, also der Datenbank „names.nsf“ im Datenverzeichnis der Domino-Server. Wer gewohnt war, die Dokumente und Dateien direkt zu bearbeiten, tut sich sicher am Anfang schwer, die einzelnen Funktionen, Dokumente und Texte im Administrator-Client wiederzufinden. Aber, wenn man sich erst einmal umgestellt hat, birgt dieses Werkzeug große Vorteile. Der Administrator kann von seinem Arbeitsplatz aus das Domino-System verwalten und hat dazu das geeignete Werkzeug. Um mit diesem Werkzeug vertrauter zu werden, soll der Administrator-Client an dieser Stelle genauer beschrieben werden.

Mai 2001 / 5. EL

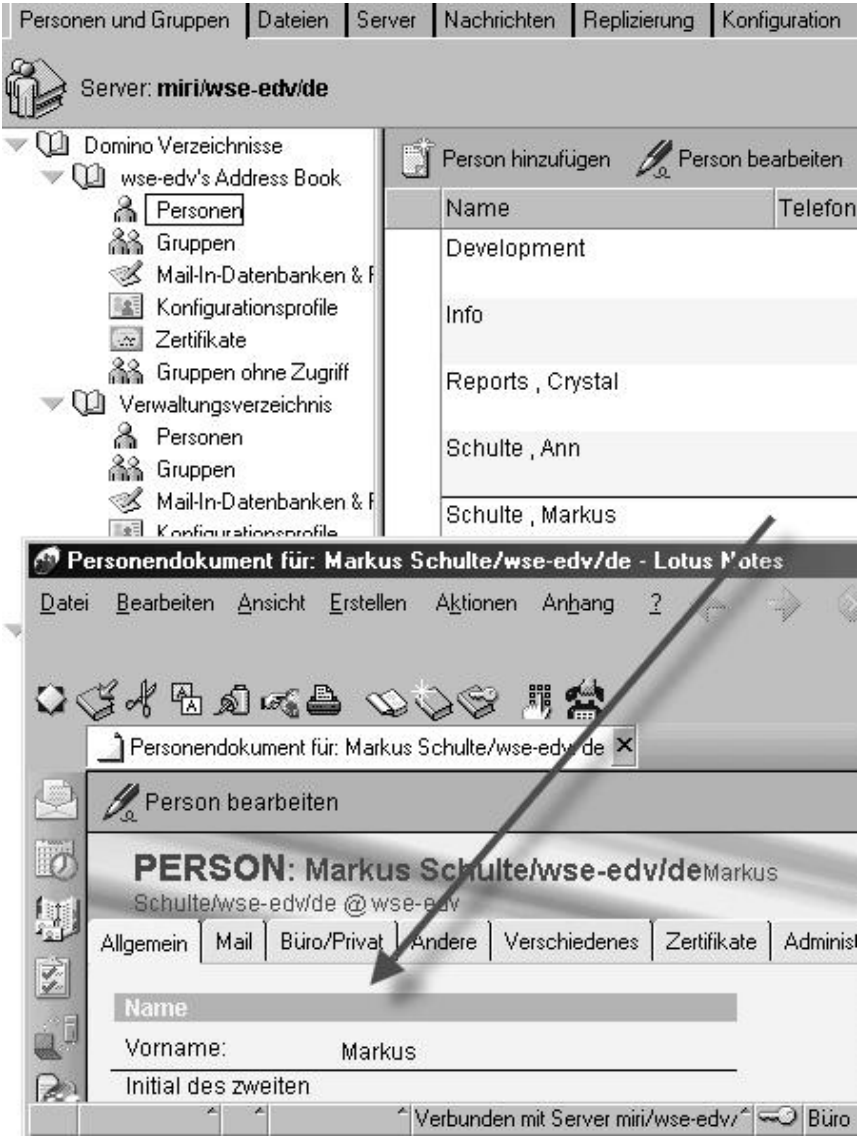
Diese Seite ist zur Zeit nicht belegt.

2.2.1 Das Menü

Das Menü im Administrator-Client ändert sich jeweils im Verhältnis zu dem ausgewählten Register. Es zeigt also andere Auswahlpositionen bei „Personen und Gruppen“, als bei „Dateien“. Dabei erscheinen die Funktionen im Wesentlichen sowohl im Menü als auch in den Werkzeugen.

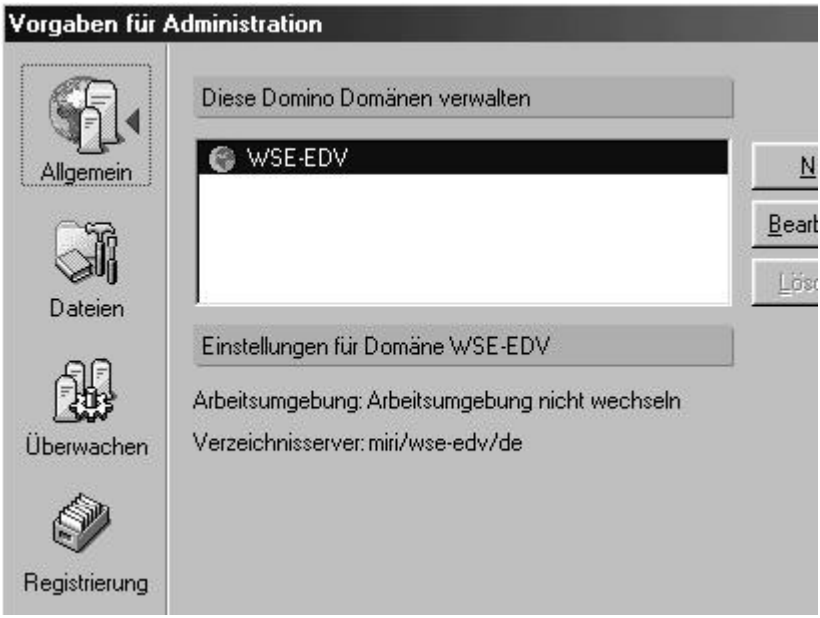
In den Menüs des Administrator-Clients sind Positionen enthalten, die nur dort zu finden sind!

Das Menü „Datei“ zeigt nur eine zusätzliche Position im Verhältnis zum Notes-Client: nämlich die Position „Server“, mit deren Hilfe der zu bearbeitende Server ausgewählt werden kann. Die Positionen „In neuem Fenster öffnen“ und „Schließen“ erscheinen nur, wenn das Register „Personen und Gruppen“ ausgewählt wird. Sie dienen zur Anzeige und zum Schließen eines ausgewählten Dokumentes.



Das Menü „Datei / In neuem Fenster öffnen“

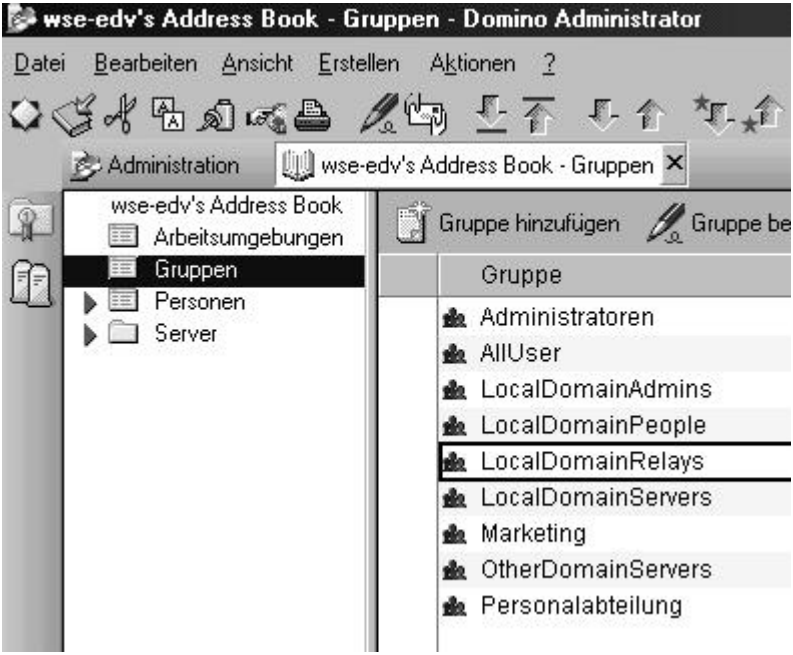
Interessant ist außerdem die Position „Vorgaben / Administration ...“.



Vorgaben Administration

Diese Position enthält wichtige Voreinstellungen zur Domäne, dem Administrations-Server, der Registrierung von Benutzern, der Server-Überwachung und zur Dateianzeige.

Nur bei ausgewähltem Register „Personen und Gruppen“ erscheint die Menüposition „Anzeigen“. Sie bezieht sich auf das Domino-Verzeichnis (names.nsf) des gerade aktuellen Servers.



Ansicht aus names.nsf

Die angebotenen Ansichten

- Agenten
- Arbeitsumgebungen
- Gruppen
- Personen
- verschiedene Server-Ansichten

werden durch das Anklicken der entsprechenden Menüposition direkt angezeigt.

Auch die Menüposition „Aktionen“ taucht nur auf, wenn das Register „Personen und Gruppen“ gewählt wurde. Hier finden sich eine Reihe von Einstellungen und Vorgaben, die sich für den Benutzer oder seine Arbeitsstation auswirken:

- **Administrations-ECL bearbeiten**
  Unter ECL versteht das Domino-System Einstellungen, die regeln, wer bzw. welches Programm bestimmte Aktionen auf der Arbeitsstation eines Benutzers durchführen darf. Über diese Menüposition wird festgelegt, welche Angaben für alle Benutzer als Vorgabe dienen. Bei der Konfiguration einer Arbeitsstation werden die Werte der Administrations-ECL kopiert und gelten so lange, bis sie über die Benutzervorgaben durch den Benutzer geändert werden. Der Administrator kann dem Benutzer das Recht nehmen, diese Einstellungen zu ändern.

- **Admin.-Rollen zur Zugriffskontrollliste hinzufügen**
  Aktiviert die Rollen in der Zugriffskontroll-Liste des Domino-Verzeichnisses.

- **Delegationsberechtigungen für alle Einträge**
- **Domino-Verzeichnis-Profil bearbeiten**
  Für die Domino-Domäne befindet sich im Domino-Verzeichnis ein Verzeichnisprofil, das Vorgabewerte enthält, die z. B. bei der Erstellung von Servern verwendet werden.
- **Profil entfernen**
- **Person löschen**
- **In persönliches Adressbuch kopieren**
- **Ausgewählte Person erneut zertifizieren**
  Diese Position wird verwendet, um die Zertifizierung einer ID-Datei zu verlängern.
- **Internet-Zertifikat zu den ausgewählten Personen hinzufügen**
  Ist die Domino-Zulassungsstelle als Internet-Zertifizierer eingerichtet, so können über diese Menüposition Personen mit einem Internet-Zertifikat ausgestattet werden.
- **Ausgewählte Personen umbenennen**
  Mehrere Personen über den Administrationsprozess umbenennen.
- **Kennwortfelder festlegen**
  Kennwortüberprüfung für die ausgewählten Personen einrichten. Die Kennwörter dieser Personen müssen dann in einem festen Rhythmus geändert werden.

- **In Ordner verschieben**
  Im Domino-Verzeichnis können Ordner erstellt und mit Personen gefüllt werden.

- **Aktualisieren auf ein sicheres Internet-Kennwortformat**
  Die Verschlüsselung der gespeicherten Internet-Kennwörter verbessern.

- **Mail-Datei verschieben**
  Mail-Datenbank eines Benutzers auf einen anderen Domino-Server verschieben.

In der Menüposition „Administration" finden sich die Namen der Register wieder. Zusätzlich sind dort die Menüpositionen aufgeführt.

- **Server-Liste aktualisieren** (für die aktuelle oder alle Domänen)

- **Server zur Favoritenliste hinzufügen**
  Einen Server als Lesezeichen in den Lesezeichen-Ordner „Favoriten" einfügen.

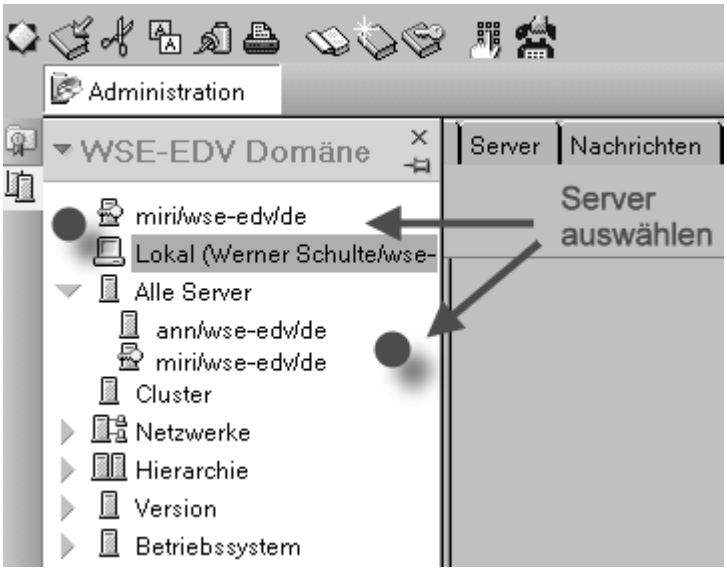
Je nach ausgewähltem Register sind in dem Menü gleichen Namens die Positionen aufgeführt, die sich auch unterhalb der Werkzeugleiste befinden.

Mai 2001 / 5. EL

Diese Seite ist zur Zeit nicht belegt.

2.2.2 Server-Verwaltung

Der Administrator-Client startet mit dem zuletzt verwendeten Server. Soll ein anderer Server ausgewählt werden, so kann in den Lesezeichenseiten „Favoriten“ und „Domäne“ eine Auswahl getroffen werden.



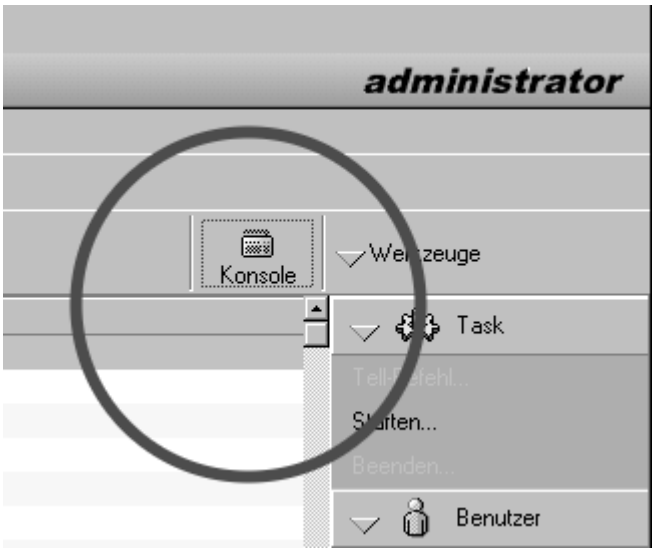
Server-Auswahl

Alle Register beziehen sich auf den ausgewählten Server. Damit alle Server der Domäne angezeigt werden, kann im Menü „Administration“ die Position „Serverliste aktualisieren“ aufgerufen werden.

Diese Seite ist zur Zeit nicht belegt.

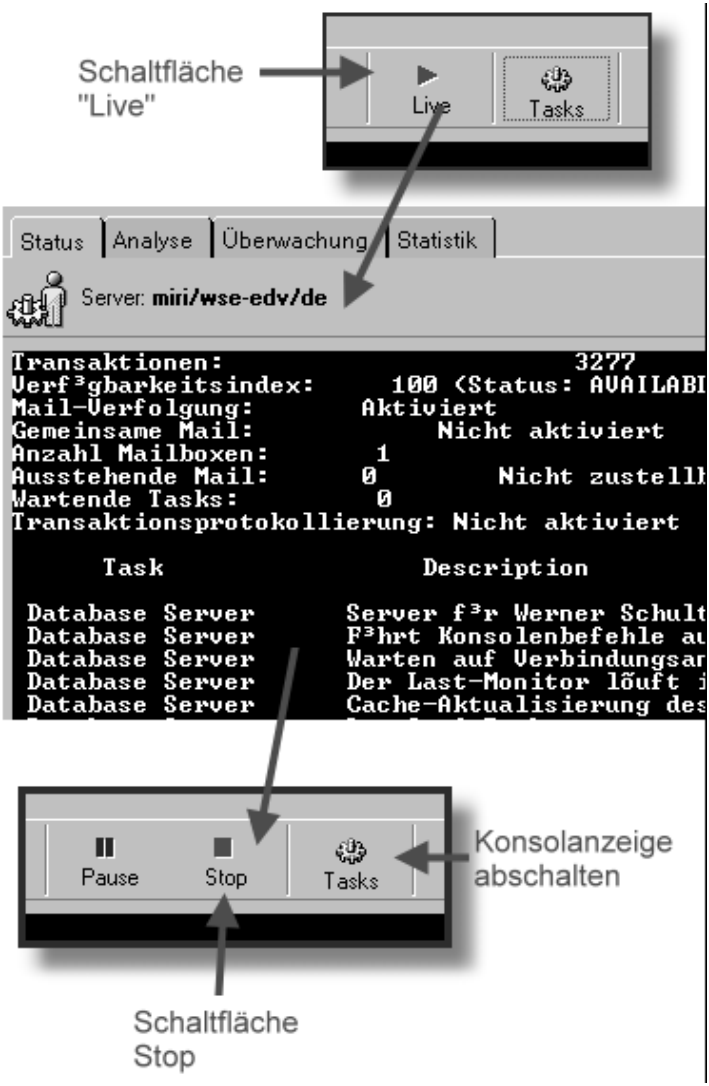
2.2.3 Die Server-Konsole

Eine wichtige Quelle für Informationen im Domino-System stellt die Konsole der Server dar. Hier werden alle wichtigen Aktionen und Meldungen eines Servers angezeigt. Die Konsole des aktuellen Servers wird im Administrator-Client angezeigt, wenn sie im Register „Server“ über die Schaltfläche „Konsole“ und danach über „Live“ gestartet wird.



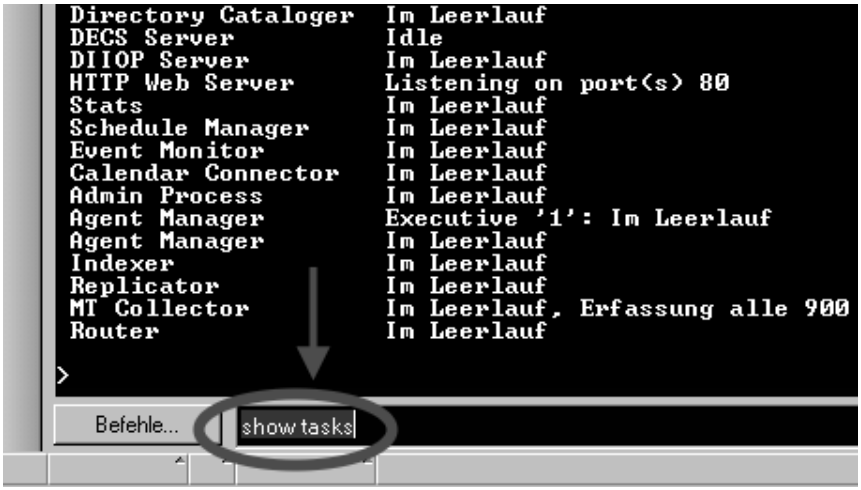
Die Schaltfläche Konsole

Mit der Schaltfläche „Stop“ kann die Anzeige beendet und mit „Pause“ unterbrochen werden.



Starten und Stoppen der Server-Konsole

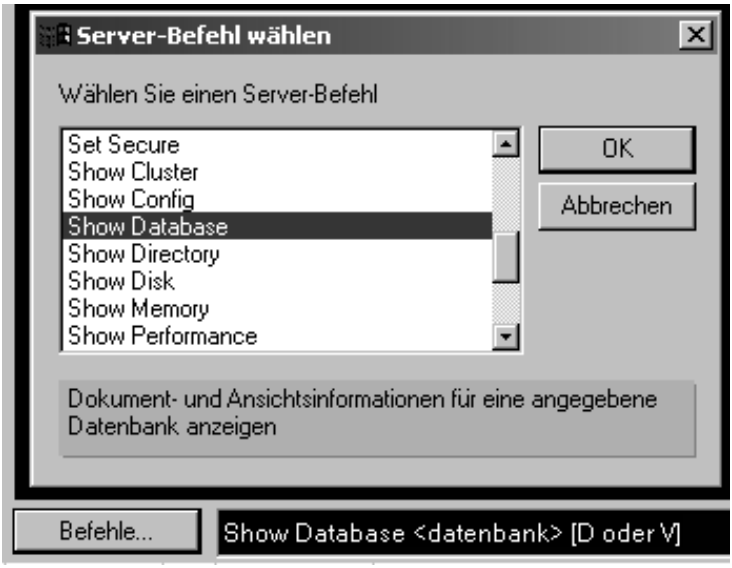
In der Befehlszeile am unteren Rand der Konsole können Befehle für den Server eingegeben werden.



Konsolbefehle

Die Befehle werden an den Server gesendet und dort ausgeführt. Die Anzeige erfolgt dann wieder im Konsolfenster. Die einzelnen Server-Befehle sind im Anhang aufgelistet.

Eine Liste der Server-Befehle kann über die Schaltfläche „Befehle“ angezeigt werden.



Server-Befehle

Leider fehlt an dieser Stelle eine Schaltfläche „Hilfe“, die Erläuterungen zu den einzelnen Befehlen bietet.

Die Schaltfläche „Tasks“ führt zurück zur Anzeige der Server-Prozesse.

❶❷❸ Ausführungsschritte:

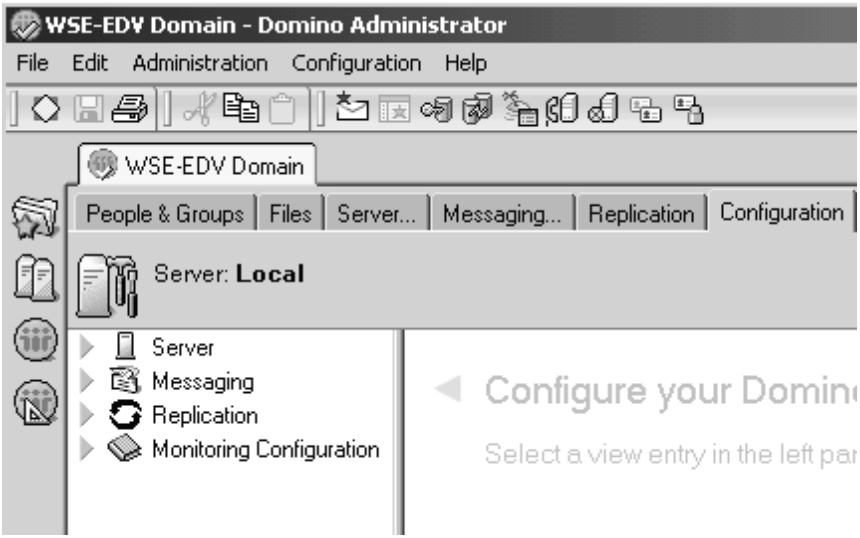
1. Administrator-Client starten
2. Server in „Favoriten“ oder „Domäne“ auswählen
3. Register „Server“ anklicken
4. Schaltfläche „Konsole“ verwenden
5. Mit Hilfe der Schaltfläche „Live“ die Konsolanzeige starten
6. Befehl in der Befehlszeile eingeben und mit „Enter“ zum Server senden
7. Über die Schaltfläche „Stop“ die „Live“-Anzeige beenden
8. Mit Hilfe der Schaltfläche „Tasks“ zur Standard-Anzeige des Servers zurückkehren

❶❷❸

Diese Seite ist zur Zeit nicht belegt.

2.3 Der Administrator-Client unter Release 6

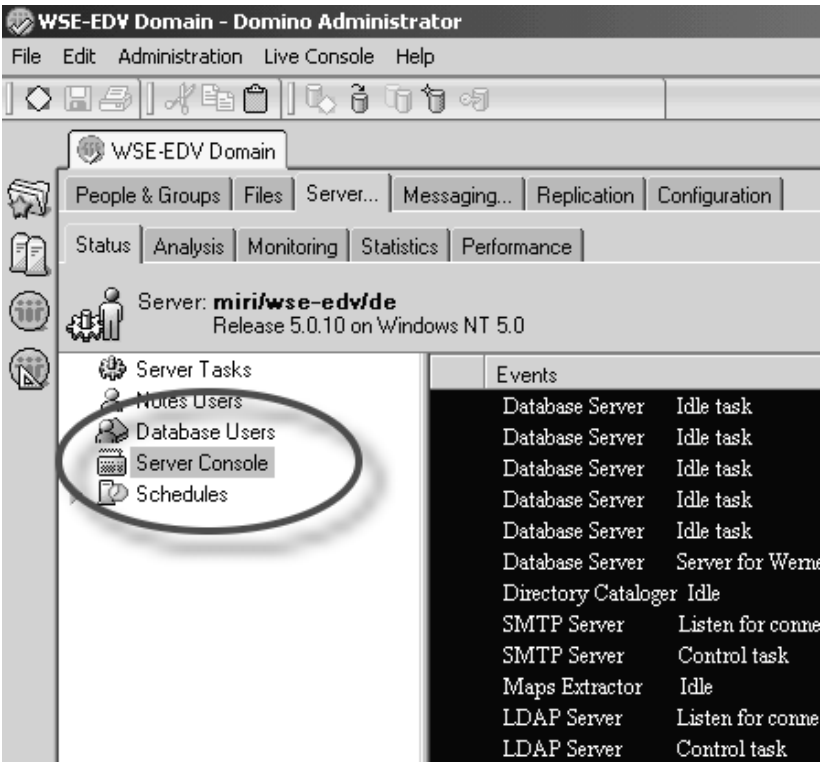
Der Administrator-Client hat auf den ersten Blick die wenigsten Änderungen im Verhältnis zu der Vorgängerversion aufzuweisen. Nur bei näherem Hinsehen findet man die Erweiterungen. Die einzige Änderung, die sofort auffällt, besteht in den Leitseiten zu den Registern, die aber nicht mehr auftauchen, sobald man die Register benutzt hat.



Leitseite – „Konfiguration“

Die Symbolleiste wurde an den Notes-Client angepasst und mit entsprechenden Symbolen versehen. Die wichtigsten Änderungen sind:

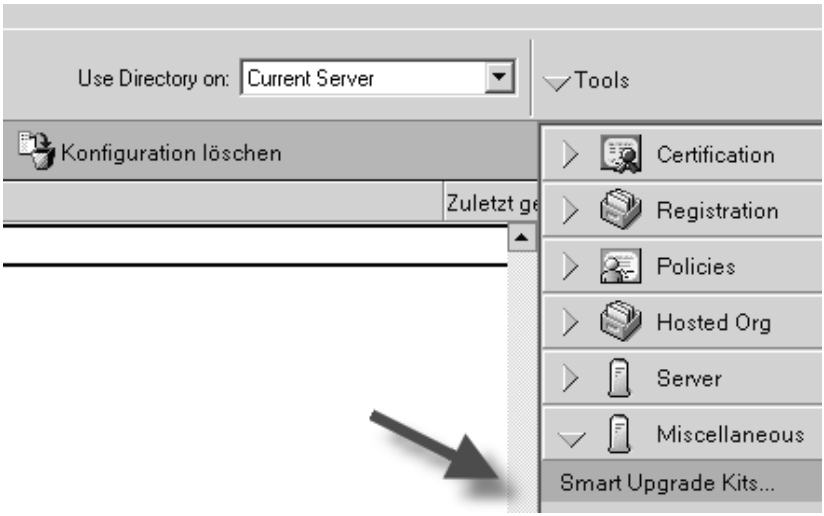
- **Ausbau der Konsole**
  Die Domino-Konsole ist als Java-Applet ausgebaut worden, das fast unter jedem Betriebssystem eingesetzt werden kann.



Server-Konsole

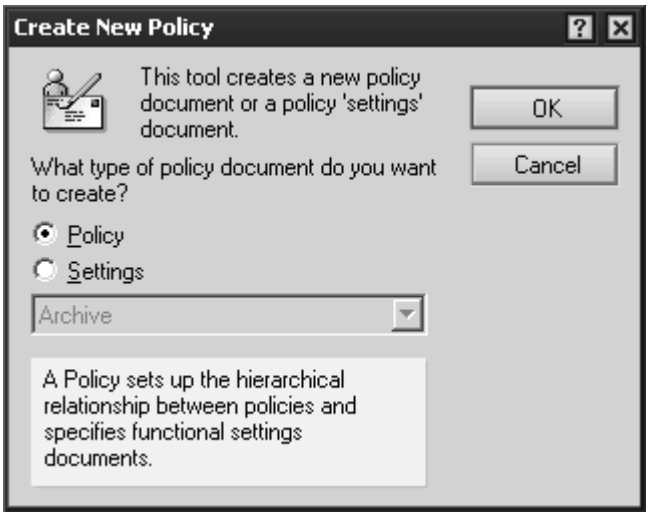
Der Aufruf wurde in die linke Gliederung des Server-Registers verlagert.

- **SmartUpgrade**
  unterstützt die Aktualisierung der Notes-Client-Software auf den einzelnen Arbeitsstationen über eine Verwaltungsdatenbank sowie über Richtliniendokumente. Der Benutzer löst dabei den Aktualisierungsprozess selbst aus.



SmartUpgrade

- **Richtlinien**
  Ein umfangreiches System an Richtlinien und Einstellungen erlaubt es dem Administrator, die Einflussnahme des Benutzers auf die Oberfläche des Notes-Clients zu beeinflussen.



Richtlinien

- **Erweiterte Protokollierung**
  der Server-Aktivitäten in Bezug auf Mail-Routing, Replikation, Agenten und Datenbanken.

- **Neue Dokumente für die Steuerung des Webservers**
  Protokollbeschränkungen für HTTP, WebDAV-Unterstützung, Vorgaben für Benutzer, die über das Internet auf den Domino-Server zugreifen.

- **Erweiterungen bei der Steuerung des Mail-Routings**
  Filter zur Reduzierung eingehender E-Mails (Spam-Filter).

- **IBM Tivoli Analyzer für Lotus Domino**
  kann als Tool im Rahmen von Tivoli verwendet werden. Dazu muss man allerdings eine spezielle zusätzliche Lizenz erwerben.

Das Werkzeug „Administrator-Client“ wurde also weiter ausgebaut und als Steuerungsinstrument verbessert. Die Vielzahl der Steuerdatenbanken und Steuerdokumente führt allerdings dazu, dass viele Einstellungen auch über den Administrator-Client nicht einfach aufzufinden sind.

Diese Seite ist zur Zeit nicht belegt.

2.4 Die Serververwaltung über Browser

Mit Release 6 hat IBM die Möglichkeiten des Administrator-Clients über Browser (Webadmin-Client) erheblich erweitert. Das ist wohl vor allem deshalb geschehen, um Administratoren, die nicht aus dem Domino-Umfeld stammen, die Arbeit mit Domino-Servern zu erleichtern. Um Lotus Domino-Server über einen Internet-Browser administrieren zu können, müssen die folgenden Voraussetzungen geschaffen werden:

- Netzwerkverbindung über TCP/IP,
- Browser ab einer bestimmten Version,
- bestimmte Server-Tasks müssen gestartet sein,
- der Benutzer muss auf die Datenbank „webadmin.nsf“ über ausreichende Zugriffsrechte verfügen.

Diese Seite ist zur Zeit nicht belegt.

2.4.1 Netzwerkverbindung über TCP/IP

Der Zugriff auf den Webadmin-Client erfolgt über das Netzwerkprotokoll TCP/IP. Die einfachste Möglichkeit, um zu testen, ob die Verbindung zum Server über TCP/IP funktioniert, ist ein „Ping"-Befehl von der MS-DOS-Eingabeaufforderung aus: Starten Sie ein MS-DOS-Fenster und geben Sie den Befehl „ping <hostname>" oder „ping IP-Adresse" ein. Wenn sich der Web-Client auf dem gleichen Rechner befindet, kann auch über die lokale Adresse 127.0.0.1 auf den Lotus Domino-Server zugriffen werden.

Diese Seite ist zur Zeit nicht belegt.

2.4.2 Mindestanforderungen an den Internet-Browser

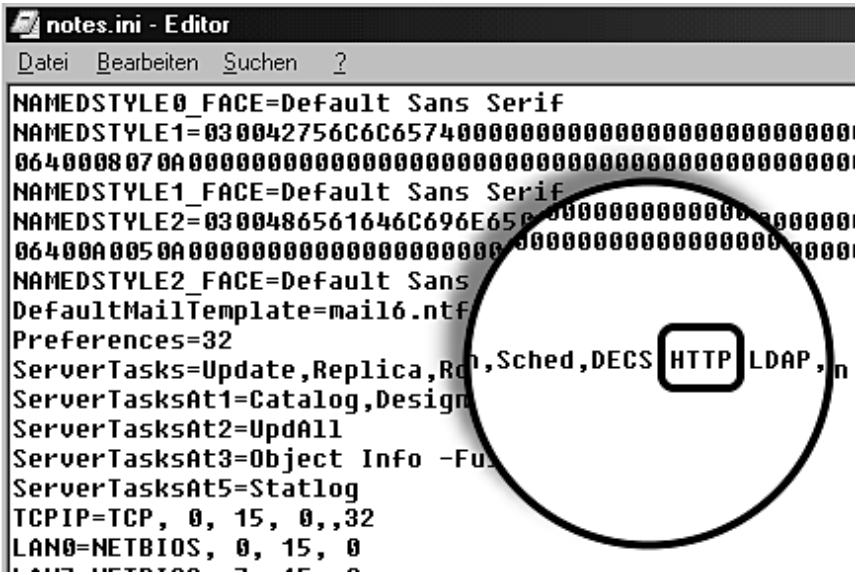
Als Client für die Benutzung des Webadministrators müssen beim Microsoft Internet Explorer die Version 5.5 und beim Netscape Navigator mindestens die Version 4.7x verwendet werden. Andernfalls bricht der Lotus Domino-Server die Verbindung mit einer Fehlermeldung ab.

Diese Seite ist zur Zeit nicht belegt.

2.4.3 Die Prozesse „HTTP“, „AdminP“ und „Certifier“ müssen gestartet sein

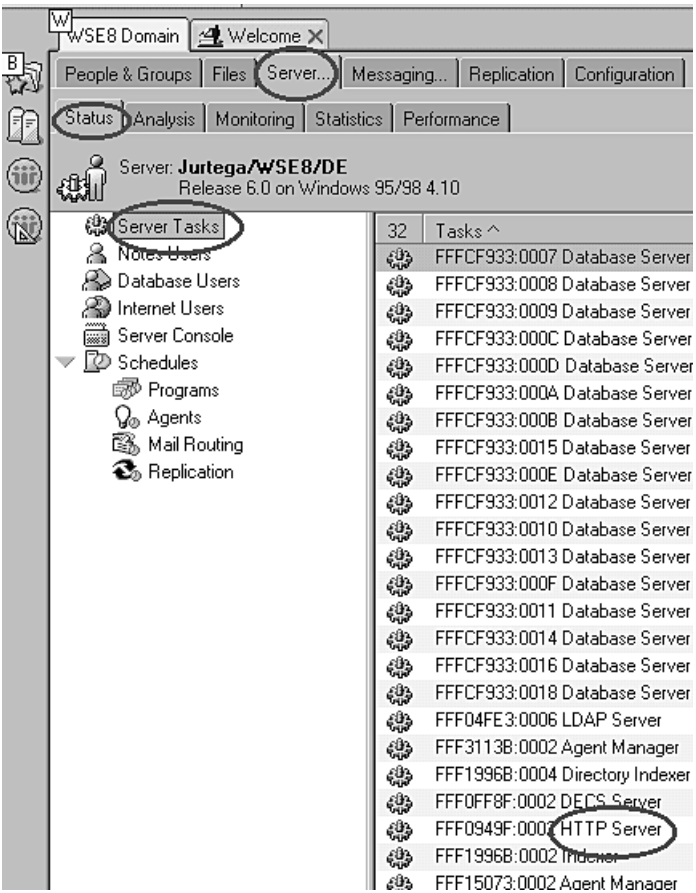
Für das Funktionieren des Webadministrator-Clients sind drei Tasks notwendig, die konfiguriert und gestartet sein müssen.

- HTTP
  Für die Bereitstellung des HTTP–Protokolls und die Umwandlung der Informationen aus den Lotus Notes-Datenbanken in HTML-Befehle ist der HTTP-Task notwendig. Damit der Task jedes Mal zusammen mit dem Lotus-Domino-Server gestartet wird, muss er in der Datei „notes.ini“ in die Zeile “ServerTasks” eingefügt werden.



Der HTTP-Task in der Datei „notes.ini“

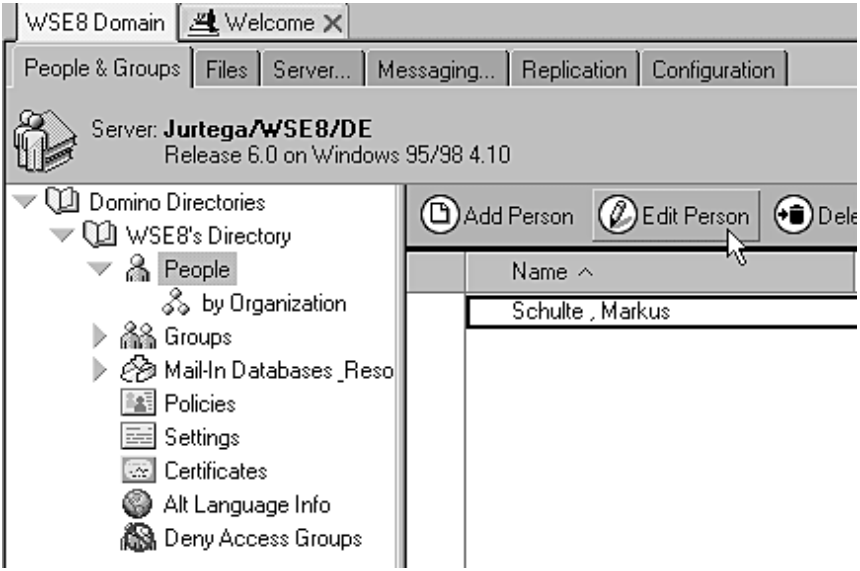
Die Datei „notes.ini“ befindet sich im Programmverzeichnis des Lotus Domino-Servers. Um zu kontrollieren, ob der HTTP-Task korrekt gestartet wurde, kann im Domino-Administrator-Client über die Reiter „Server / Status“ und dann im linken Fenster durch einmaliges Anklicken des Punktes „Server-Tasks“ der aktuelle Status aller auf dem Server laufenden Prozesse geprüft werden.



Statusprüfung der Prozesse der Server

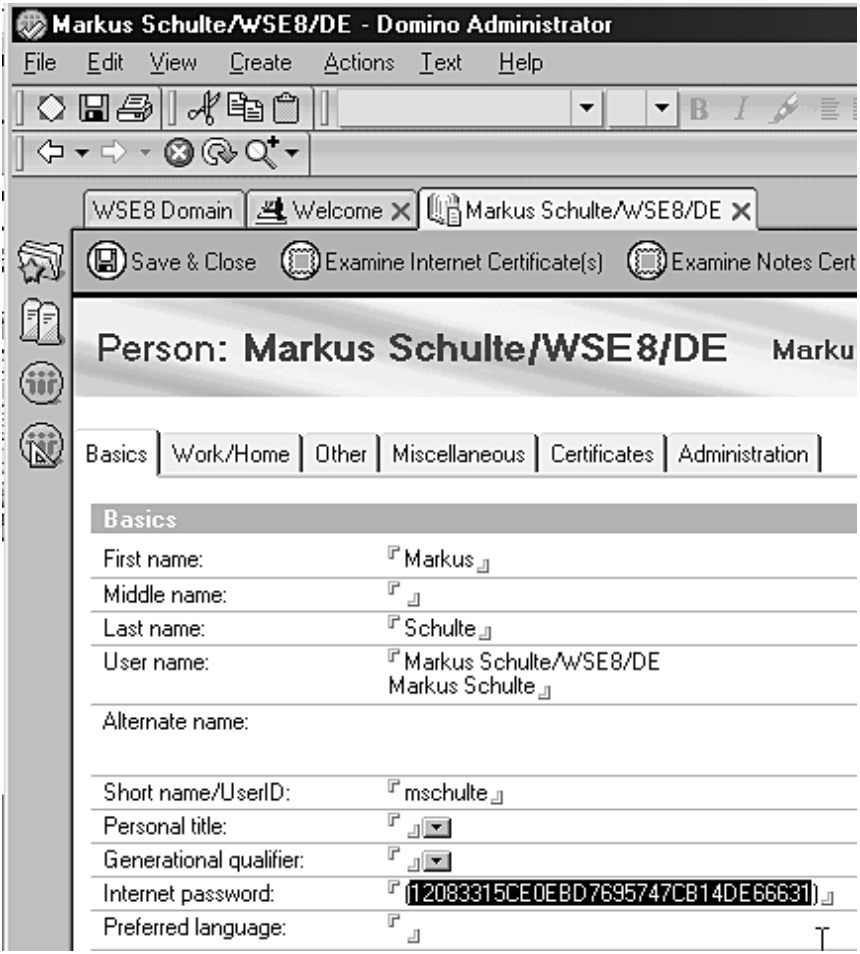
- *AdminP*
  Der Administrationsprozess „AdminP“ wird dazu verwendet, mehrere administrative Aufgaben zu automatisieren. Die Aufgabe wird vom Administrator angestoßen und der Task führt sie aus. Beispiele für seine Möglichkeiten sind die Re-Zertifizierung von Benutzer-IDs, das Umbenennen und Löschen von Referenzen auf Lotus-Benutzer und -Benutzergruppen, die Erstellung von Datenbankrepliken und das Verschieben von Datenbanken. Er muss ebenfalls gestartet sein, wenn der Webadminstrator verwendet werden soll, weil dieser auf einige Funktionen des AdminP-Prozesses zugreift. Er wird ebenfalls in die „notes.ini“-Datei eingetragen.

- *Certifier*
  Da der Zugriff auf den Server nur Personen gestattet werden soll, die sich legitimiert haben, wird der Zertifizierer-Prozess ebenfalls benötigt. Es kann nur dann ein Zugriff über einen Browser erfolgen, wenn der Benutzer sich durch ein Internet-Kennwort angemeldet hat oder der Zugriff über einen SSL-Client erfolgt. Damit die Anmeldung über das Internet-Kennwort möglich ist, muss es zunächst beim Benutzer definiert sein. Der Benutzer wird über den Reiter „People & Groups“, anschließend im linken Fenster durch Klicken auf „People“und dann durch Doppelklicken auf den Benutzer zum Bearbeiten geöffnet.



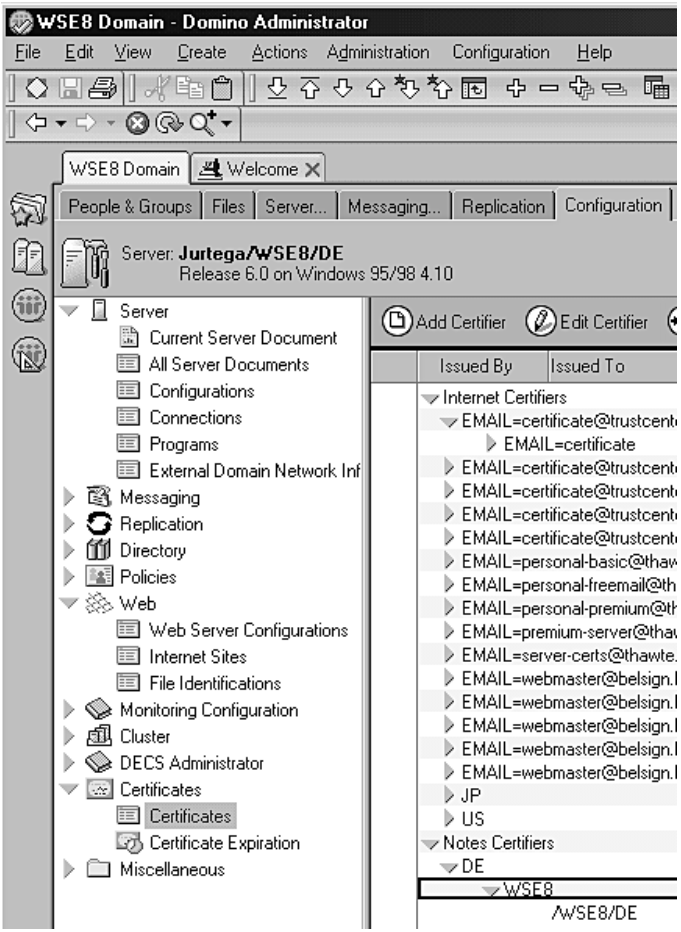
Benutzer für das Internet-Kennwort wählen

In der Maske mit den Benutzerdaten wird im Feld „Internetkennwort“ unter dem ersten Reiter „Allgemein“ das Kennwort eingetragen.



Internet-Kennwort anlegen

Für ein fehlerfreies Funktionieren des Zertifizierer-Prozesses wird als Nächstes seine Konfiguration angelegt. Dazu wird im Lotus Domino-Administrator-Client auf „Konfiguration“ geklickt. Dann wird in der Werkzeugleiste auf der rechten Seite der Punkt „Registration / Internet-Certifier“ ausgewählt.

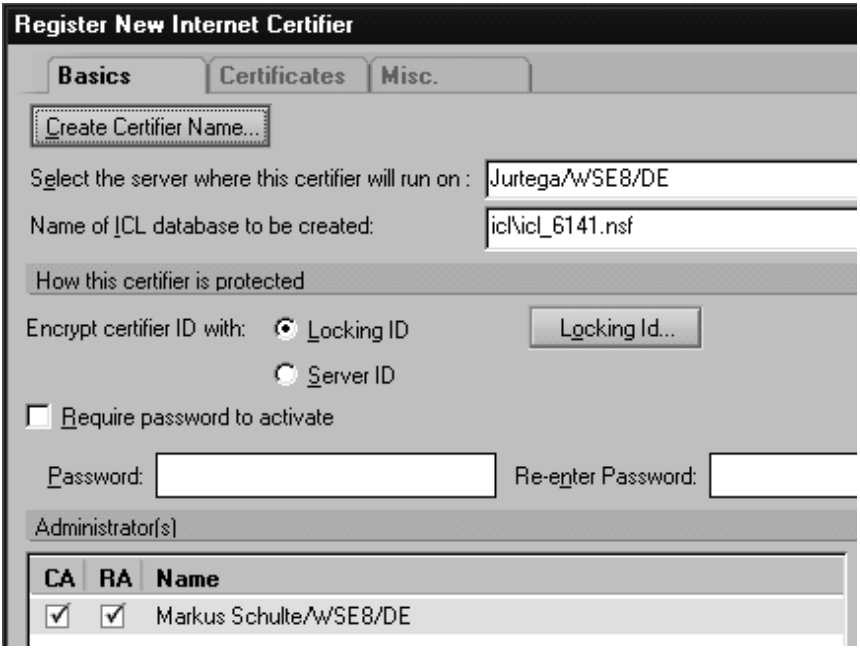


Konfiguration anlegen

In der Dialogbox, die sich darauf hin öffnet, wird der zweite Punkt „I want to register a new internet certifier that uses the CA process“ verwendet.

Registrierung des Zertifizierers

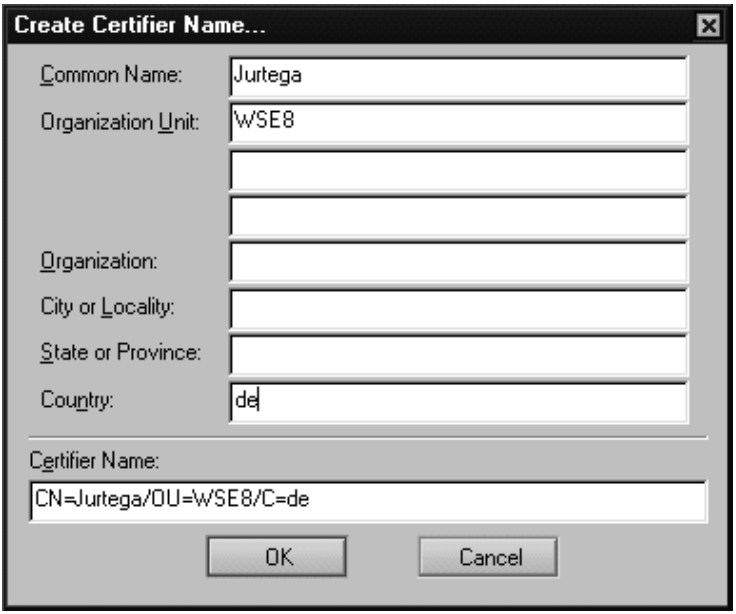
Es öffnet sich ein weiterer Dialog: „Register New Internet Certifier“.



Angaben zum Zertifizierer

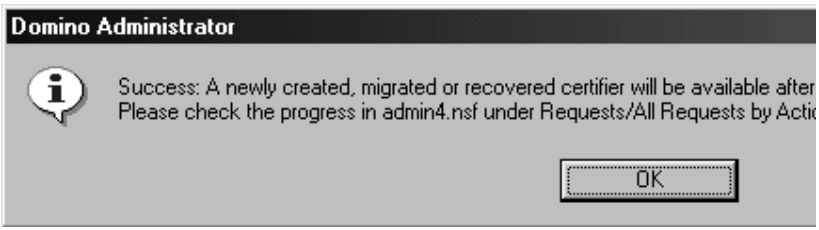
Hier sind mehrere Schritte notwendig, um eine grundlegende Konfiguration für einen Internet Certifier zu erstellen:

- Schaltfläche „Create Certifier Name“ anklicken.
- In der folgenden Dialogbox „Create Certifier Name“ wird der Name des Internet-Zertifizierers zusammengestellt. Hierfür stehen die bekannten Komponenten der hierarchischen Namensgebung von Lotus Notes zur Verfügung.



Zertifizierer-Name anlegen

- Durch Klicken auf „OK“ wird der Prozess zur Erstellung der Konfiguration gestartet, der je nach System einige Zeit laufen kann. Nach erfolgreicher Erstellung wird eine entsprechende Meldung eingeblendet.



Meldung: „Konfiguration abgeschlossen“

Diese Seite ist zur Zeit nicht belegt.

2.4.4 Eintragen des Administrators in der ACL der Webadmin-Datenbank

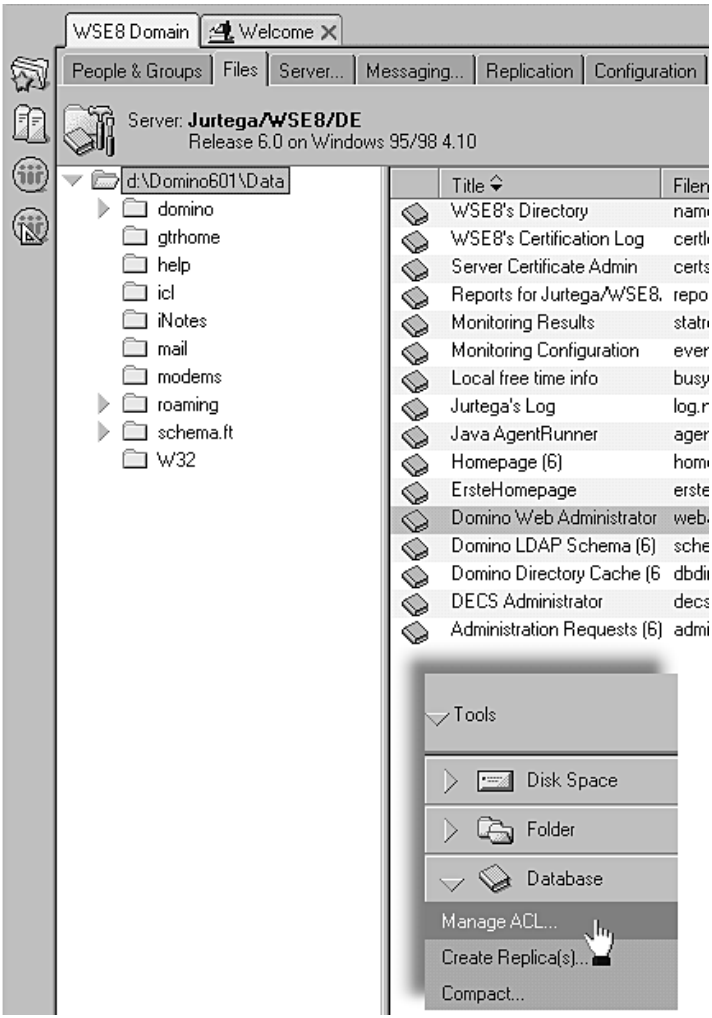
Der Web Adminstrator verwendet die Lotus Notes-Datenbank „webadmin.nsf“. Wenn der HTTP-Prozess zum ersten Mal gestartet wird, legt er automatisch die Datenbank „webadmin.nsf“ im Domino-Datenverzeichnis an. Dabei wird die bei Domino übliche Datenbanksicherheit für die Einrichtung der Zugriffskontroll-Liste dieser Datenbank verwendet. Alle, die im Feld „Administrator“ des Server-Dokuments eingetragen sind, werden in der Zugriffskontroll-Liste mit „Manager-Zugriff“ eingetragen. Falls dies beim Erstellen nicht erfolgt ist, kann über „Files“ und dann in der Werkzeugleiste mit „Datenbank / Manage ACL“ die Zugriffskontroll-Liste der „Webadmin“-Datenbank aufgerufen sowie der Name des Administrators eingetragen werden.

Damit sind alle Voraussetzungen geschaffen, damit die Administration von Domino-Servern über gängige Internet-Browser erfolgen kann.

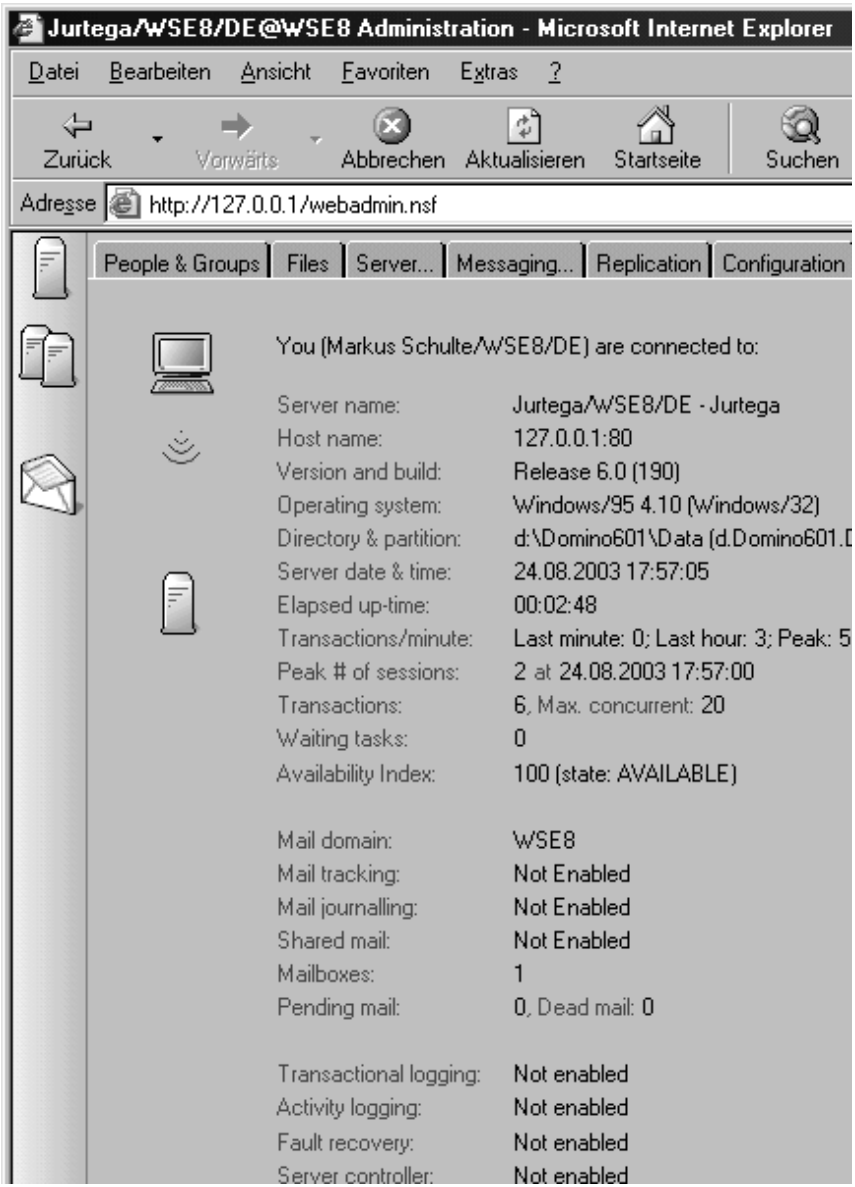
Der Zugriff auf den Webadmin-Client erfolgt mit dem Browser, indem in der Adresszeile „http:\\<hostname“ oder „IP-Adresse>/webadmin.nsf“ eingegeben wird. Nach dem Laden einiger Applets steht der Webadminstrator dann im Browser zur Verfügung.

Da auch hier die für Domino und Notes relevanten Einträge gemacht werden, setzt die Administration auch über den Browser intensive Domino-Kenntnisse voraus.

Das äußere Erscheinungsbild ist zwar an die Optik der Browser angepasst, das Wissen über die Wirkungsweise von Lotus Domino und Notes lässt sich dadurch nicht ersetzen.



Zugriffskontroll-Liste „Webadmin.nsf“ ändern



Startbild Webadministrator

Diese Seite ist zur Zeit nicht belegt.

3

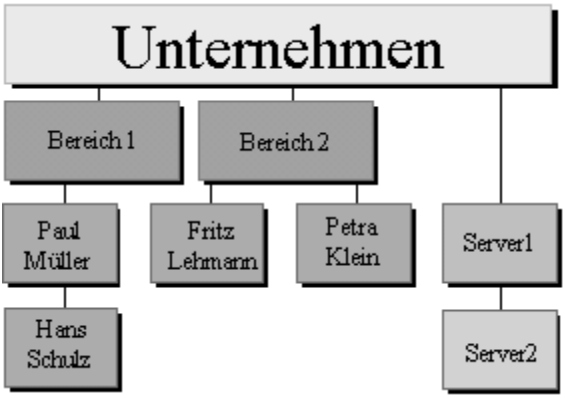
Strukturen und Hierarchien

Bevor mit der Installation begonnen werden kann, muß zunächst der Aufbau des Systems anhand der Unternehmensstruktur geplant werden. Dazu gehören:

- Domänen und hierarchische Namensgebung
- Protokolle, Netzwerke und ihre Namen
- Server und ihre Funktionen

- Replizierung und Routing
- Benutzer und Gruppen
- Anwendungen und Anwendungsentwicklung

Für die Planung des Domino-Systems empfiehlt es sich, ein Diagramm der Unternehmensorganisation als Grundlage zu nehmen.



Unternehmensorganisation

Zudem ist es erforderlich, die verschiedenen technischen Netzwerke und die möglichen Server-Standorte zu berücksichtigen. Mit Hilfe eines solchen Grobkonzeptes kann dann ein exakter Plan aufgestellt werden, der auf die unterschiedlichen Server-Funktionen ausgerichtet ist.

Für die Umsetzung sollte genau überlegt werden, ob auch zukünftige Erweiterungen im Unternehmen noch mit dem Konzept abgedeckt werden können.

3.1 Netzwerke

Für die Abbildung der technischen Netzwerke im Domino-System erhält jedes Netzwerk einen eindeutigen Namen, der in den Server-Dokumenten hinterlegt wird. Innerhalb eines solchen Netzwerkes können die Server jetzt über das Protokoll dieses Netzwerkes direkt miteinander kommunizieren. Für ein Netzwerk im Domino-System kann nur ein Protokoll verwendet werden. Wenn Server in unterschiedlichen Netzwerken miteinander kommunizieren sollen, müssen Verbindungsdokumente die Kommunikation sicherstellen.

Für ein Netzwerk unter Lotus Domino gilt also:

- je Protokoll muss ein getrenntes Netzwerk verwendet werden
- innerhalb eines Netzwerkes sind keine Verbindungsdokumente notwendig
- zwischen Server in unterschiedlichen Netzwerken ist keine direkte Kommunikation möglich
- als Netzwerkname kann das Protokoll verwendet werden

Ein Netzwerk kann auch Remote-Verbindungen beinhalten. In diesem Fall wird die Verbindung zwischen den lokalen und den externen Servern, soweit keine Standleitung besteht, für jeden Zugriff aufgebaut.

Im Rahmen von Lotus Domino können folgende Netzwerke eingesetzt werden:

- TCP/IP
- NetBIOS
- NetWare (SPX, SPXII, IPX)
- Banyan VINES
- AppleTalk

3.2 Domänen und Server

Ein Domino-System besteht aus mindestens einer Domäne, einem Netzwerk, einem Domino-Server und einer Arbeitsstation mit einem Notes-Client.

Die Domäne stellt dabei den Bereich dar, in dem die anderen Komponenten beheimatet sind. Typischerweise verwendet man deshalb den Namen des Unternehmens auch als Domänen-Namen.

Domino-Server stellen eine Sammlung von Prozessen zur Verfügung, die das Domino-System mit Daten versorgen, mit anderen Servern kommunizieren, das System überwachen und steuern.

Domino unterscheidet zwischen verschiedenen Server-Typen, wie z.B.:

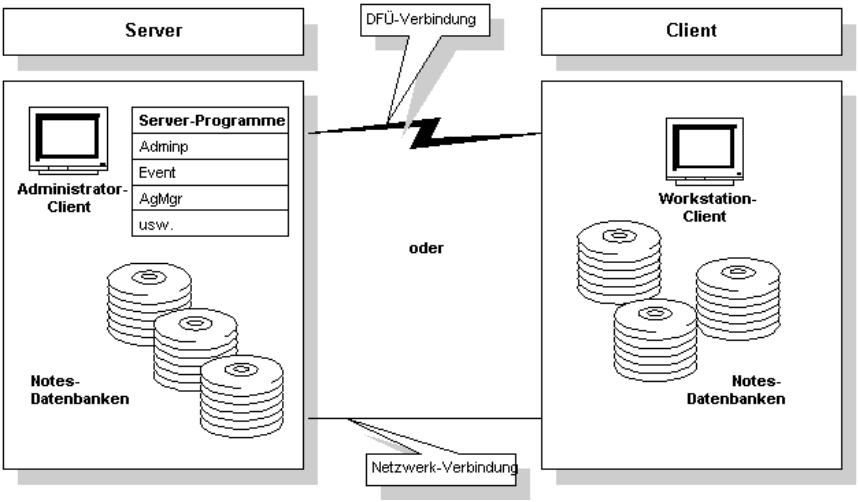
- Mail Server
- Hub Server
- Verzeichnis-Server
- Anwendungs-Server
- Durchgangs-Server

Dabei bezieht sich die Namensgebung auf den Prozess, den ein bestimmter Server vorzugsweise ausführt. Notes-Server sind heute für viele Betriebssysteme verfügbar:

- Windows2000, Windows95/98
- Apple OS

- OS/2 Warp
- verschiedene UNIX-Versionen (Aix, HP-UNIX, Solaris, Linux etc.)
- OS/400
- OS/390

Entsprechend vielseitig kann auch die Kombination von Hard- und Software in einem Domino-System sein.



Server und Clients im Domino-System

Bei den Clients hat sich die Position von Windows in den letzten Jahren sehr verstärkt.

3.3 Domäne einrichten

Der erste Schritt zur Einrichtung eines Domino-Systems besteht in der Installation eines ersten Domino-Servers. Auf diesem Server wird das Domino-Verzeichnis (Namens- und Adressbuch) eingerichtet und werden alle Steuerdokumente für den Betrieb der Domäne definiert. Zur Konfiguration und Verwaltung des Servers wird auf dem Server selbst oder aber auf einer Arbeitsstation ein Administrator-Client installiert. Danach können alle weiteren Teile des Systems in Betrieb genommen werden.

Diese Seite ist zur Zeit nicht belegt.

3.4 Software

Die Domino-Software besteht heute aus einem ganzen Bündel von Programmen. Die Server-Software wird für die oben aufgeführten Betriebssysteme als Variante geliefert und teilt sich in verschiedene Komponenten für die einzelnen Prozesse auf. Die Client-Software wird in drei Programme unterteilt:

- Notes-Client für die Nutzung von Anwendungen
- Designer-Client für die Entwicklung von Anwendungen
- Administrator-Client für die Verwaltung, Überwachung und Steuerung des Domino-Systems

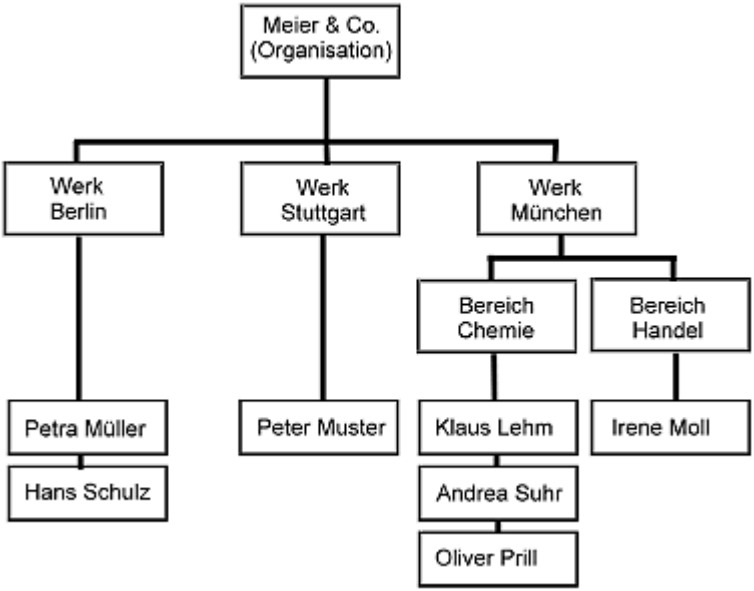
Datenbanken können sowohl auf den Servern als auch auf den Arbeitsstationen gespeichert werden. Nur bei Datenbanken auf Servern ist ein gemeinsamer Datenzugriff möglich.

Sollen lokal gespeicherte Datenbanken inhaltlich anderen Benutzern zugänglich gemacht werden, so wird eine Kopie (Replik) dieser Datenbank auf dem Server erstellt, die dann von einem anderen Benutzer gelesen oder bearbeiten werden kann. Die Synchronisation der Inhalte solcher Repliken erfolgt über den Replikationsmechanismus von Lotus Domino.

Diese Seite ist zur Zeit nicht belegt.

3.5 Namensvergabe

Domino verwendet ein hierarchisches Namenssystem. An oberster Stelle steht die Domäne. Darunter können bis zu vier Ebenen zur Untergliederung eingerichtet werden. Auf der untersten Ebene werden dann die einzelnen Benutzer angesiedelt. Die Benutzernamen müssen unter Berücksichtigung der Hierarchie eindeutig sein.



Organisationsebenen

Die einzelnen Ebenen der Organisation werden in den Namen mit aufgeführt. Der Name von Oliver Prill aus dem Schaubild lautet z.B. Oliver Prill/Chemie/München/Meier/de. Die Namensbestandteile werden durch „/“ getrennt. Da bei der Installation

eines Domino-Servers die Namen angegeben werden müssen, ist es wichtig, die Namensvergabe vor der Installation des ersten Servers zu regeln.

4

Server-Installationen

Die wichtigste Entscheidung bei der Installation eines Servers ist die Wahl der Hardware und des Betriebssystems. Da die Server-Software für alle gängigen Systeme verfügbar ist, wird diese Entscheidung von technischen und wirtschaftlichen Gesichtspunkten abhängen.

Technisch gesehen, sind vor allem die Anzahl der Benutzer und die Art der einzusetzenden Anwendungen ausschlaggebend für ein System. Auch die bereits eingesetzte Hard- und Software sind wichtige Faktoren, weil damit Investitionen und Know-how verbunden sind. Lotus Domino kann zwar mit jedem heute üblichen

System aufgebaut werden, die Nutzung wird aber umso aufwendiger, je mehr Benutzer auf ein solches System zugreifen und je höher die Anforderungen der Anwendungen an Systemressourcen und Netzbandbreite sind.

Außerdem müssen Sicherheitsüberlegungen einbezogen werden. Das gilt sowohl im Hinblick auf die Sicherheit der Daten als auch im Hinblick auf die Ausfallsicherheit des Systems.

Die wirtschaftlichen Faktoren sind einmal die Investition in Hard- und Software, zum anderen aber auch Folgekosten in Form von Wartung und personeller Betreuung.

Welche Entscheidung auch gefällt wird, Lotus Domino kann jederzeit auf eine andere Plattform übernommen und dem Wachstum des Unternehmens angepasst werden.

Die Installation eines Domino-Servers ist für alle Plattformen sehr ähnlich und unterscheidet sich im Bereich der systemabhängigen Komponenten. Die Vorbereitungen der Systemvoraussetzungen unterscheiden sich wesentlich stärker und erfordern zum Teil umfangreiche Vorbereitungen für die Installation.

Domino-Installation

Der Start ist vom jeweiligen Betriebssystem abhängig und beeinflusst im wesentlichen das Kopieren der Dateien auf die Festplatte des Rechners. Die Konfiguration des Servers erfolgt über den Notes-Client des Administrators. Die eigentliche Installation gliedert sich in zwei Hauptschritte:

- Einspielen der Lotus-Domino-Software
- Konfiguration des Servers

Diese Seite ist zur Zeit nicht belegt.

4.1 Installation unter Windows

Die verschiedenen Windows-Versionen wurden in letzter Zeit einander immer mehr angeglichen. Es soll deshalb an dieser Stelle lediglich die Installation unter Windows95/98 beschrieben werden.

4.1.1 Voraussetzungen

Die Hardware-Anforderungen liegen zunächst im Rahmen der heute üblichen Server-PCs. Da sie aber sehr stark von der Anzahl der Benutzer und den eingesetzten Anwendungen abhängen, können hier nur allgemeine Aussagen gemacht werden. Lotus Domino braucht im Server-Bereich starke Ressourcen, wenn die Zahl der aktiven Benutzer größer wird. Ein PC-Server kann deshalb nur dann sinnvoll verwendet werden, wenn die Anforderungen an Benutzerzahl und Ausfallsicherheit nicht sehr hoch eingestuft werden. Da unter Windows auch der Notes- und der Administrator-Client auf dem Server-PC installiert werden können, sind für die Installation zunächst kein Netzanschluss und kein Browser erforderlich.

Diese Seite ist zur Zeit nicht belegt.

4.1.2 Die Installation

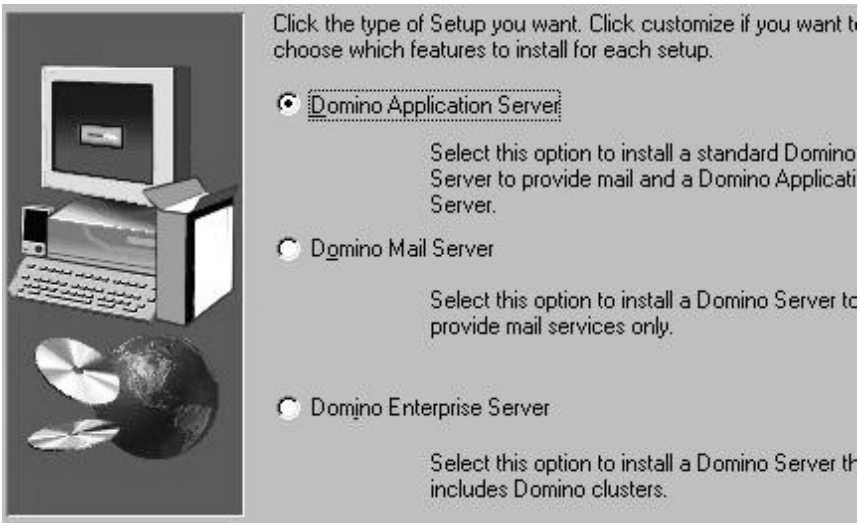
Die Server-Software wird auf CD-ROM geliefert und kann direkt von der CD, aber auch vom Netzwerk aus installiert werden. Das Setup-Programm führt nach den Begrüßungs- und Lizenzvertragsdialogen zur Abfrage von Name und Firma.

Sollen mehrere Server auf einem Rechner installiert werden, so muss das Feld „Installation für partitionierte Server“ bei der Installation jedes dieser Server markiert werden.

Der nächste Dialog legt fest, wohin die Dateien kopiert werden sollen.

Domino-Verzeichnisse

Seit Release 5.0 unterscheidet Domino bei den Verzeichnissen zwischen Server und Client. Die Standardverzeichnisse lauten dabei „\Lotus\Domino\...“ für den Server und „\Lotus\Notes\...“ für den Client. Das hat viele Vorteile, kann aber auch hin- und wieder verwirrend sein (wenn der Administrator auf dem Server-Gerät arbeitet), weil Datenbanken, die auf dem Server liegen, konsequent im Domino-Verzeichnis bzw. dessen Unterverzeichnissen und solche, die lokal liegen, konsequent im Notes-Verzeichnis bzw. dessen Unterverzeichnissen gespeichert werden. Ein wichtiger Vorteil dieser Namenskonvention liegt darin, dass die Dateien „notes.ini“ mit wichtigen Informationen zum aktuellen Programmablauf für Server und Client in getrennten Verzeichnissen gespeichert werden.Es folgt das Fenster für die Auswahl zwischen verschiedenen Server-Arten.



Server-Arten

Die Server-Arten in der Übersicht:

- Domino Anwendungs-Server

  Enthält Mail- und Anwendungsdienste.

- Domino Mail Server

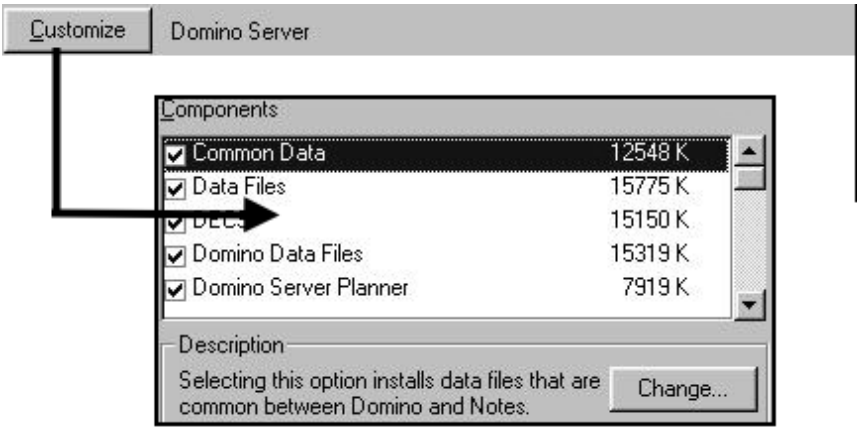
  Enthält nur die Mail-Funktionen von Lotus Domino.

- Domino Enterprise Server

  Erweitert Lotus Domino um die Möglichkeit, Cluster zu verwenden. Es können mehrere Server so miteinander verbunden werden, dass bei Überlastung eines Servers ein anderer dessen Aufgaben mit übernehmen kann. Damit wird die Auslastung optimiert und Ausfallsicherheit gewährleistet.

Die Standard-Installation bei kleinen und mittleren Systemen bildet der Domino-Anwendungs-Server. Für große Systeme, die Clustering benötigen, kommt der Domino Enterprise Server zum Einsatz. Für die Server-Typen sind unterschiedliche Lizenzen erforderlich, die sich im Preis z.T. erheblich unterscheiden.

Über die Schaltfläche „Anpassen“ können einzelne Komponenten ausgewählt werden.



Benutzerdefinierte Installation

Normalerweise sollten alle Dateien, die zum entsprechenden Server-Typ gehören auch installiert werden. Ob Domino unter WindowsNT als Service gestartet werden soll, kann, muss aber nicht an dieser Stelle entschieden werden.

Nach Auswahl der Gruppe für das Startmenü werden die Dateien von der CD in die gewählten Verzeichnisse kopiert. Nach Beendigung dieser ersten Installationsphase sollte das Gerät neu gebootet werden.

4.1.3 Die Konfiguration

In der ersten Phase der Installation erfolgt lediglich das Erstellen der Dateien auf dem Zielgerät. Die inhaltliche Installation beginnt in dem Moment, in dem der Server zum erstenmal gestartet wird.

Meldung des Servers beim 1. Start

Der Server startet in dieser Situation den Notes-Client und dieser wiederum die Konfigurationsdatenbank. Die Konfiguration erfolgt in vier Schritten, zwischen denen über Pfeiltasten hin- und hergewechselt werden kann. Die Schaltfläche „Speichern und Schließen“ ermöglicht das Sichern des aktuellen Konfigurationsstandes. Dieser Stand kann nach einem erneuten Starten der Konfiguration weiterbearbeitet werden.

Der erste Bildschirm beschränkt sich auf die Frage, ob der erste oder ein weiterer Server einer Domäne konfiguriert werden soll.

Server SetUp, Schritt 1

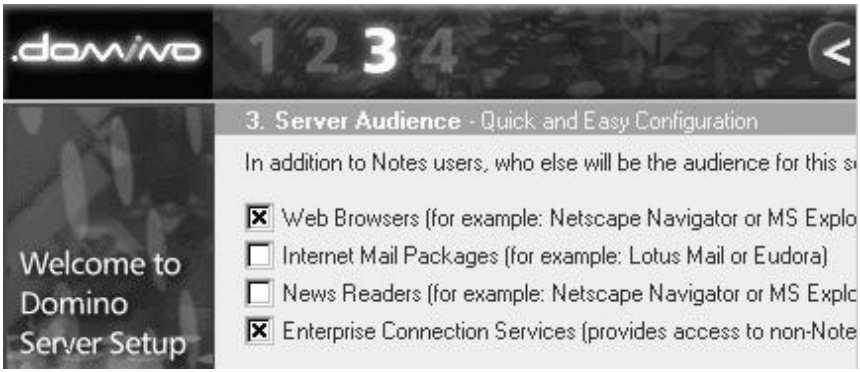
Der erste Server einer Domäne unterscheidet sich von den übrigen dadurch, dass er das Domino-Verzeichnis der Domäne enthält. Wir wählen an dieser Stelle den ersten Server aus und klikken „Weiter“ an.

Server SetUp, Schritt 2 – Einfache Konfiguration

Das Konfigurationsprogramm ermöglicht zwei unterschiedliche Vorgehensweisen:

- die schnelle und einfache Konfiguration
- die Konfiguration für Experten

Die „Einfache Konfiguration“ vermeidet einzelne Parameter und versucht über allgemein formulierte Fragen die Standardkonfiguration auf die gewünschte Mail- und Datenanbindung hin anzupassen. Diese Methode wird für die Installation des ersten Servers einer Organisation empfohlen.



Server SetUp, Schritt 3 – Einfache Konfiguration

Bereits mit Version 4.6.x hat Lotus auch Browser-Funktionalitäten in Domino integriert. Sie werden nun bei der Server-Konfiguration mit eingerichtet. Die einfache Zusammenarbeit mit anderen Mail-Systemen ist inzwischen eine Stärke von Domino und Notes.

Um diese Offenheit bieten zu können, benötigt Domino im Zuge der Konfiguration die Angabe, welche Client-Typen bzw. welche Arten von Benutzern mit dem Server arbeiten und kommunizieren sollen.

- Web-Browser

  Markieren, wenn auf den Server mit Web-Clients (Netscape Navigator, Microsoft Internet Explorer etc.) zugegriffen werden soll.

- Internet-Mail-Programme

  Markieren, wenn auf den Server mit den Clients anderer Mail-Systeme (ccMail, Exchange etc.) zugegriffen werden soll.

- News Reader

  Markieren, wenn der Server als News-Server arbeiten soll.

- Enterprise Connection Services (DECS)

  Markieren, wenn auf externe Datenbanken zugegriffen werden soll.

Es können mehrere Felder angekreuzt werden.

Auch der abschließende 4. Schritt der Installation versucht mit wenigen Parametern auszukommen. Über die Schaltfläche „Bearbeiten“ wird das Fenster zum Editieren freigegeben. Lediglich die Angaben zur Domäne, zum Server und zum Administrator werden benötigt, um die Konfiguration abzuschließen.

Server SetUp, Schritt 4 – Einfache Installation

Der Name des Zertifizierers bildet die oberste Zulassungsstelle der Domäne (cert.id) und ist für die Zulassung aller weiteren Zulassungsstellen, Server und Personen die Basis.

Bevor Sie das Konfigurationsprogramm verlassen, sollten Sie die Kennwörter auf der 4. Seite überprüfen, gegebenenfalls ändern, genau notieren und an einer sicheren Stelle (Tresor) hinterlegen.

Gehen wir noch einmal zurück zu Schritt 2 und wählen wir jetzt die erweiterte Installation.

Server SetUp, Schritt 2 – Erweiterte Konfiguration

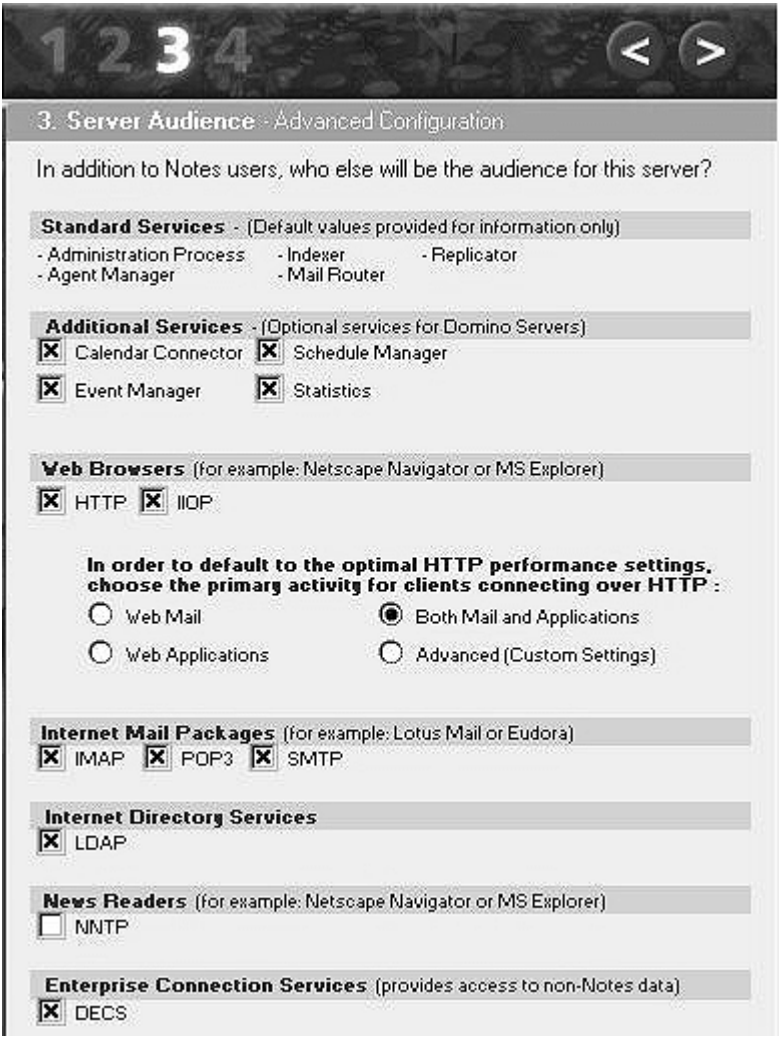
Hier werden jetzt die einzelnen Parameter sichtbar, die bei der einfachen Installation automatisch erfüllt werden:

- Standardprozesse

  Die Standardprozesse werden in jedem Fall installiert.

- Zusätzliche Prozesse

  Die Prozesse Freie-Zeit-Verwaltung, Zeitplan-Manager, Event-Manager und Statistik-Prozess können einzeln ausgewählt werden.



Server SetUp, Schritt 3 – Erweiterte Konfiguration

- Web-Browser

  HTTP-Prozess und IIOP-Unterstützung können aktiviert werden, damit Web-Browser auf Domino-Datenbanken zugreifen können.

- Internet-Mail

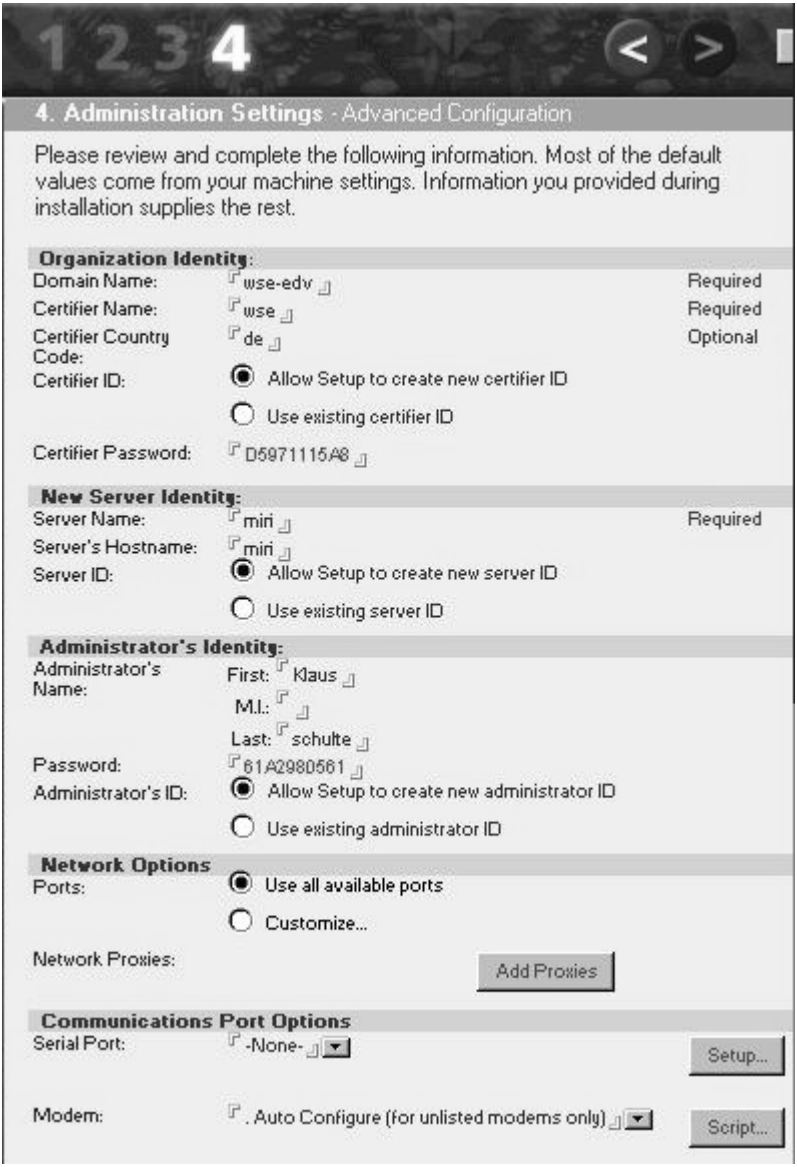
  Verwendung der Internet-Protokolle SMTP, POP3 und IMAP.

- News

  Verwendung des NNTP-Protokolls zum Austausch von Informationen mit News-Servern.

- DECS

  (Enterprise Connection Services) verbindet Domino mit relationalen Datenbanken.



Server SetUp, Schritt 4 – Erweiterte Konfiguration

Im vierten Schritt werden zusätzlich die Netzwerkoptionen angezeigt:

- Organisation

  Der Name der Domäne und der Zulassungsstelle wird in der Regel gleich der des Unternehmens sein. Ist bereits eine Cert-ID vorhanden, kann diese verwendet werden.

- Server

  Nicht zu lange Namen verwenden, sie müssen häufig geschrieben werden. Soll der Server im Domino-System einen anderen Namen tragen als im Netz, kann der Host-Name sich vom Server-Namen unterscheiden.

- Name des Administrators

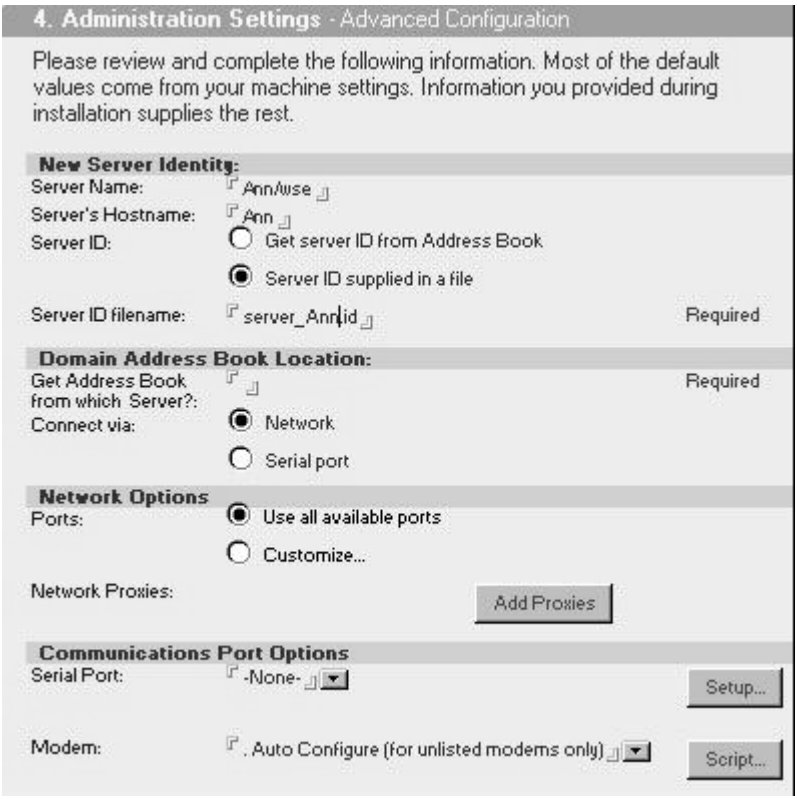
- Netzwerkoptionen und Anschlüsse

  Anschlüsse und Modems können aber auch noch später konfiguriert werden.

Die Kennwörter sollten jetzt notiert und an sicherer Stelle aufbewahrt werden. Damit ist die Server-Installation abgeschlossen.

4.1.4 Zusätzlichen Server installieren

Die Installation eines weiteren Servers erfolgt analog zur Installation des ersten Servers. Bei der Startmaske der Konfiguration wird jetzt ausgewählt, dass es sich um einen weiteren Server handelt.



Zusätzlicher Server - Schritt 4

Im Rahmen dieser Installation wird kein neues Domino-Verzeichnis (names.nsf) und keine neue Zulassungsstelle (Cert.id) erstellt. Lediglich die Angaben zum Server werden benötigt.

4.2 Installation auf der iSeries (AS/400)

Mit dem Anspruch, Lotus Notes auf den gängigsten Plattformen verfügbar zu halten, hielt dieses Groupeware-Produkt auch Einzug in die AS/400-Welt und wurde seit der ersten verfügbaren Version OS/400 V4R2M0 in Verbindung mit dem Notes Release 4.6 ständig weiterentwickelt.

Es bestehen enge Abhängigkeiten zwischen der Kompatibilität des jeweiligen OS/400 Release-Standes zu der auf der iSeries zu installierenden Domino-Release-Version.

Welches Domino-Release unter welcher OS/400-Version unterstützt wird, ist jeweils den aktuellen IBM Web-Seiten zu entnehmen.

Die iSeries hat sich seit der ersten verfügbaren Native-Domino-Version zu einem leistungsfähigen Domino-Server entwickelt. Auf einem einzigen System können mehrere 1.000 Domino-User gleichzeitig arbeiten.

Auf einer iSeries lassen sich mehrere Domino-Server parallel installieren. In der Anfangsphase von Lotus Notes auf der AS/400 war nur eine „Quasi"-AS/400-Version auf dem Integrierten xSeries-Adapter (frühere Bezeichnungen FSIOP, IPCS oder auch Integrierter Netfinity-Server) verfügbar. Wer nicht besondere Gründe für den Einsatz von Lotus Notes auf diesem integrierten PC-Server hat, sollte sich für die „echte" iSeries-Lösung – die Domino-Native-Installation – entscheiden.

Die Installation von Domino erfolgt als Lizenzprogramm und kann, wie die Basis-Konfiguration auch, über OS/400-Befehle

oder verschiedene grafische Installationsmethoden durchgeführt werden.

Der Domino-Server selbst läuft in einem eigenen Domino-Subsystem (DOMINOxx). Bei der Installation mehrerer Domino-Server auf einem iSeries-System wird für jeden Domino-Server ein eigenes Subsystem erstellt.

Bis zur Release-Version 6.0.2 konnten auf einer iSeries bzw. in einer Logischen Partition zwar mehrere Domino-Server parallel installiert werden, diese konnten aber immer nur über einen Domino-Release-Stand verfügen. Seit dem Release 6.0.3 besteht mit „Multiversioning“ die Möglichkeit, auf einer iSeries in einer logischen Partition mehrere Domino-Server mit unterschiedlichen Release-Ständen parallel zu installieren.

In Verbindung mit weiteren Middleware-Produkten wie Tivoli und WebSphere kann der Einsatz von Domino noch weiter optimiert werden.

4.2.1 Systemvoraussetzungen

Nachfolgende Voraussetzungen müssen erfüllt sein, um Lotus Domino native auf der iSeries zu installieren:

Die Anforderungen an die iSeries variieren je nach Domino Release. Aktuelle Informationen dazu bieten die IBM Web-Seiten.

Nachfolgende Anforderungen dienen als Grundlage für die Installation von Domino 6 auf iSeries.

4.2.1.0 Systemvoraussetzungen Release 6

- AS/400-RISC-Modell
- OS/400, mind. Version V5
- mindestens 512 MB Hauptspeicher für Lotus Domino
- ausreichend Plattenplatz auf der iSeries (mind. 1,5 GB)
- TCP/IP (57xx-TC1)
- Host-Server (57xx-SS1 Option 12)

Die Voraussetzungen für frühere Domino-Release-Versionen weichen in Bezug auf den erforderlichen Hauptspeicher und den erforderlichen Plattenplatz ab. Diese sind geringfügig niedriger, als die Mindestanforderungen von Release 6.x.

Zudem belegt jeder aktive Notes-User Hauptspeicherplatz und Plattenplatz, der von der Art der Notes/Domino-Nutzung abhängt.

Es sei noch einmal betont, dass die Angaben zu den einzelnen Punkten als Mindestvoraussetzungen angesehen werden sollten, was insbesondere für die Angabe zum Hauptspeicher gilt.

Es wird dringend empfohlen, den aktuellsten PTF-Stand des OS/400 installiert zu haben. Sind alle Voraussetzungen erfüllt, kann mit der Installation des Domino-Servers begonnen werden.

Bei Unsicherheiten, ob die Voraussetzungen erfüllt sind, empfiehlt sich der Einsatz des Workload-Estimators, ein Web Tool, mit dem unter Angabe bestimmter Parameter das Sizing unter anderem auch für Domino auf iSeries durchgeführt werden kann.

Weitere Informationen zu diesem Tool finden Sie in Kapitel 4.2.1.4!

Diese Seite ist zur Zeit nicht belegt.

4.2.1.1 Überprüfen der installierten Software

Wenn der Stand der installierten Software unbekannt ist, so können Sie die derzeit installierte Software z.B. über das Menü „Mit Lizenzprogrammen arbeiten“ (GO LICPGM) ermitteln. Wählen Sie in diesem Menü den Punkt 10 (Installierte Software anzeigen) aus und Sie erhalten eine Übersicht über alle Lizenzprogramme. Neben dem Lizenzprogrammnamen können Sie nach Betätigen der Befehlstaste „F11“ den Stand des derzeit installierten Releases erkennen. Ist dieser nicht mindestens V4R2M0, so ist die Installation des Domino-Servers nicht möglich. Anderenfalls prüfen Sie in dieser Anzeige, ob die weiteren Software-Voraussetzungen erfüllt sind:

Installierte Lizenzprogramme anzeigen
System: S44R3881

Installiertes Lizenzprogramm	Release	Beschreibung
5769SS1	**V4R3M0** L00	OS/400 – Bibliothek QGPL
5769SS1	V4R3M0 L00	OS/400 – Bibliothek QUSRSYS
5769SS1	V4R3M0 L00	Betriebssystem IBM OS/400
5769SS1	V4R3M0	OS/400 – Erweiterte Basisunterstützung
5769SS1	V4R3M0	OS/400 – Online-Informationen
5769SS1	V4R3M0	OS/400 – Extended Base Directory Support
5769SS1	V4R3M0	OS/400 – S/36- und S/38-Umstellung
5769SS1	V4R3M0	OS/400 – IBM System /36-Umgebung
5769SS1	V4R3M0	OS/400 – IBM System /38-Umgebung
5769SS1	V4R3M0	OS/400 – Bibliothek mit Beispielprogrammen
5769SS1	V4R3M0	OS/400 – AFP-Verträglichkeitsschriftarten
5769SS1	V4R3M0	OS/400 – *PRV CL-Compiler-Unterstützung
5769SS1	V4R3M0	OS/400 – S/36-Umstellungsunterstützung

Weitere ...

Eingabetaste —> Weiter

F3=Verlassen F11=Option anzeigen F12=Abbrechen F19=Marken anzeigen

Installierte Lizenzprogramme anzeigen

Nach erneutem Drücken der „F11“-Taste wird in der zweiten Spalte die „Produktoption“ angezeigt. Blättern Sie so weit, bis Sie die Option 12 des Lizenzprogrammes 5769-SS1 sehen. Dies ist der Host-Server. Suchen Sie anschließend nach dem Eintrag „5769-TC1“, den TCP/IP-Funktionen unter OS/400.

Installierte Lizenzprogramme anzeigen
System: S44R3881

Lizenz-programm	Produkt-option	Beschreibung
5769SS1	**12**	**OS/400 – Host-Server**
5769SS1	13	OS/400 – System Openness Includes
5769SS1	14	OS/400 – GDDM
5769SS1	16	OS/400 – Ultimedia System Facilities
5769SS1	20	OS/400 – Advanced 36
5769SS1	21	OS/400 – Erw. Unterstützung f. Landessprachen
5769SS1	22	OS/400 – ObjectConnect
5769SS1	30	OS/400 – QShell Interpreter
5769SS1	31	OS/400 – Domain Name System
5769SS1	32	OS/400 – Directory Services
5769SS1	34	OS/400 – Digital Certificate Manager
5769PM1	*BASE	Performance Management/400
5769PW1	*BASE	App Dev ToolSet für AS/400 - SEU

Weitere ...

Eingabetaste —> Weiter

F3=Verlassen F11=Status anzeigen F12=Abbrechen F19=Marken anzeigen

Check Installation Host-Server

Installierte Lizenzprogramme anzeigen
System: S44R3881

Lizenz-programm	Produkt-option	Beschreibung
5769PW1	1	App Dev ToolSet für AS/400 - Andere
5769QU1	*BASE	Query für AS/400
5769RG1	*BASE	ILE RPG für AS/400
5769RG1	1	IBM System /36-kompatibles RPG II für AS/400
5769RG1	2	IBM System /38-kompatibles RPG III für AS/400
5769RG1	5	RPG für AS/400
5769RG1	6	*PRV ILE RPG für AS/400
5769ST1	*BASE	DB2 Query Mgr and SQL DevKit für AS/400
5769TC1	***BASE**	**TCP/IP Connectivity Utilities für AS/400**
5763XD1	*BASE	Client Access für Windows 95/NT
5769XW1	*BASE	AS/400 Client Access-Familie für Windows

Ende

Eingabetaste —> Weiter

F3=Verlassen F11=Status anzeigen F12=Abbrechen F19=Marken anzeigen

Check Installation TCP/IP

Den PTF-Stand Ihrer Maschine können Sie mit dem Befehl „DSPPTF“ ermitteln. Geben Sie dazu den Befehl „DSPPTF LICPGM(5769SS1)“ ein. In der folgenden Anzeige suchen Sie nach dem ersten Eintrag, der mit TC beginnt. Die folgenden fünf Ziffern geben den Stand des PTFs wieder (für die Mindestvoraussetzung unter V4R2M0 wäre dies TC98045).

PTF-Status anzeigen
System: S44R3881

Produkt-ID . . . . . : 5769SS1
IPL-Quelle . . . . . : ##MACH#B
Release der Basisoption . . : V4R3M0 L00

Auswahl eingeben und Eingabetaste drücken.
5=PTF-Zusatzinformationen anzeigen 6=PTF-Begleitschreiben drucken
8=PTF-Begleitschreiben anzeigen

Auswahl PTF-ID	Status	IPL-Aktion
TC99131	**Temporär angelegt**	Keine
TC99054	Ersetzt	Keine
TC98349	Ersetzt	Keine
TC98279	Ersetzt	Keine
TC98230	Ersetzt	Keine
TC98202	Ersetzt	Keine
TA99131	Temporär angelegt	Keine
		Weitere ...

F3=Verlassen F11=Alternative Sicht anzeigen F17=Listenanfang bei
F12=Abbrechen

Überprüfen des PTF-Standes

4.2.1.2 Überprüfen der TCP/IP-Konfiguration

Die Kommunikation zwischen dem Domino-Server und den Notes-Workstations sowie anderen externen Ressourcen läuft über TCP/IP. Damit der Domino-Server erfolgreich eingerichtet und konfiguriert werden kann, muß TCP/IP auf dem System konfiguriert und aktiviert sein.

Um dies zu überprüfen, gehen Sie wie folgt vor:

Im Menü „TCP/IP konfigurieren“ (Befehl CFGTCP) ermitteln Sie zunächst die Schnittstellen-Informationen. Wählen Sie dazu Punkt 1 „Mit TCP/IP Schnittstellen arbeiten“ aus. Suchen Sie nun nach einem Eintrag „*LOOPBACK“. Ist außer dem Eintrag „*LOOPBACK“ kein weiterer Eintrag vorhanden, so ist TCP/IP nicht eingerichtet. Anderenfalls ist TCP/IP wahrscheinlich eingerichtet. Prüfen Sie dies aber nochmals genau nach.

Installierte Lizenzprogramme anzeigen
System: S44R3881

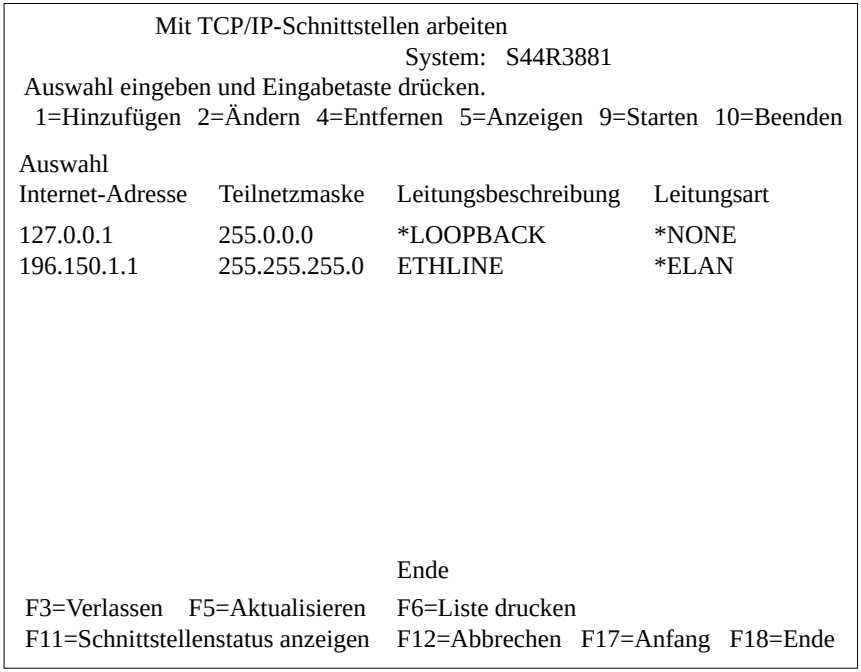
Lizenz-programm	Produkt-option	Beschreibung
5769PW1	1	App Dev ToolSet für AS/400 - Andere
5769QU1	*BASE	Query für AS/400
5769RG1	*BASE	ILE RPG für AS/400
5769RG1	1	IBM System /36-kompatibles RPG II für AS/400
5769RG1	2	IBM System /38-kompatibles RPG III für AS/400
5769RG1	5	RPG für AS/400
5769RG1	6	*PRV ILE RPG für AS/400
5769ST1	*BASE	DB2 Query Mgr and SQL DevKit für AS/400
5769TC1	***BASE**	**TCP/IP Connectivity Utilities für AS/400**
5763XD1	*BASE	Client Access für Windows 95/NT
5769XW1	*BASE	AS/400 Client Access-Familie für Windows

Ende

Eingabetaste —> Weiter

F3=Verlassen F11=Status anzeigen F12=Abbrechen F19=Marken anzeigen

Check Installation TCP/IP



Überprüfen der TCP/IP-Konfiguration

Anmerkung: „XX“ in der Bezeichnung der Lizenzprogramme (z.B. 57xx-TC1) ist ein Platzhalter für die Version des Betriebssystems.

4.2.1.3 Installationsvorbereitung

Neben der eigentlichen Installation und Konfiguration des Domino-Servers sind noch einige Vorbereitungen zu treffen:

- Prüfen, ob die AS/400 die Mindestvoraussetzungen erfüllt.
  - Das Benutzerprofil, das für die Installation verwendet wird, muss die erforderlichen Berechtigungen aufweisen.
  - Für die Software-Installation sind als spezielle Berechtigungen erforderlich:
  - *ALLOBJ (Zugriff auf alle AS/400-Objekte)
    –› *SECADM (Sicherheitsverwaltung)
- Für die Konfiguration sind als spezielle Berechtigungen erforderlich:
  - *ALLOBJ (Zugriff auf alle AS/400-Objekte)
  - *SECADM (Sicherheitsverwaltung)
  - *IOSYSCFG (Geräte- und Übertragungskonfiguration)
    –› *JOBCTL (Jobkontrolle)
- Es wird empfohlen, die Installation mit dem Benutzer QSECOFR durchzuführen.
- Es muss sichergestellt sein, daß die TCP/IP-Verbindungen auf der AS/400 eingerichtet und auch aktiv sind.
- Festlegen, ob es sich bei dem zu installierenden Server um den ersten oder um einen zusätzlichen Server in Ihrer Organisation handelt.

Mit der Einführung von Lotus Domino auf der AS/400 standen Lotus und die IBM vor dem Problem, dass man unter Umständen zwei Gruppen von Systemadministratoren ansprechen musste. Das sind auf der einen Seite die „Alt-AS/400-Anwender“, die die Administration und Konfiguration der AS/400 mittels der guten alten „Green-Screen“-Oberfläche (der 5250-Oberfläche) durchführen - und andererseits diejenigen, die das System AS/400 als Server im Einsatz haben und weniger die 15250-Oberfläche als vielmehr die grafische Oberfläche in Form einer Windows-Oberfläche (Client-Acces in Verbindung mit dem Operations Navigator) verwenden wollen. Um diesen Anforderungen Rechnung zu tragen, wurden zwei Konfigurationsmethoden entwickelt:

1. über eine 5250-Oberfläche mittels des Befehles CFGDOMSVR

2. unter Verwendung des AS/400 Operations Navigators von einer Workstation aus. Der Operations Navigator konfiguriert den Domino-Server über eine Konfigurationsdatenbank. Der PC, von dem aus dieses Verfahren angewendet werden soll, muss ein WIN95-, WIN98- oder WIN /NT-Rechner sein und über Client Access und Operations Navigator verfügen. Weiterhin ist natürlich eine Verbindung zur AS/400 erforderlich.

Diese Seite ist zur Zeit nicht belegt.

4.2.2 Die AS/400 Domino-Software

Mit dem Erscheinen der Version 6 von Domino wurden einige Änderungen im Installationsprozess auf der iSeries vorgenommen.

Die Lizenzprogramm-Nummer von Domino 4 und Domino 5 lautet: 5769-LNT.

Ab dem Domino Release 6 ändert sich diese Nummer:

- Domino 6.0.x trägt die Lizenzprogramm-Nummer 5733-LD6.
- Domino 6.5 trägt die Lizenzprogramm-Nummer 5733-L65.

Zu beachten ist auf der iSeries, dass das Release 6 von Domino mindestens die OS/400-Version V5RxMx erfordert.

Neben einigen funktionalen Erweiterungen wurde mit Release 6 auch die Unterstützung von einigen Features zurückgezogen:

- Integration über OS/400 Mail Server Framework (MSF) / Any Mail.
  - Alternativ lassen sich andere TCP/IP-Schnittstellen für SMTP verwenden.
- Keine Unterstützung mehr für Directory Synchronisation.
- Keine Unterstützung von Domino auf dem OS/400 HTTP-Server.
  - Neue Unterstützung über den Apache HTTP-Server.
- Keine landesspezifischen Installationsauswahlen.

4.2.2.0.1 Lizenzprogramm-Optionen

Die Installation von Domino für iSeries besteht aus verschiedenen (bis auf die *BASE Option) wahlweise zu installierenden Optionen.

Die zur Verfügung stehenden Optionen unterscheiden sich zwischen den Release-Funktionen 4 und 5 und den Release-Versionen 6.

Die bisher unter Release 4 und 5 verfügbaren sieben Lizenzprogramm-Optionen wurden unter Release 6 zu zwei Lizenzprogramm-Optionen zusammengefasst, wobei die bisherige Option 6 (HiTest C API) nicht mehr unterstützt wird.

Die „Advanced Services“, die im Release 5 unter der Option 7 installiert werden konnten, sind im Release 6 in die Base-Option integriert. Das iSeries Navigator Plug-In wurde ebenfalls in die Base-Option integriert.

4.2.2.0.2 Optionen unter Release 4 und 5

Unter den Release Versionen 4 und 5 stehen nachfolgende Optionen für die Installation zur Verfügung. Die *BASE Option ist in jedem Fall zu installieren; sie ist Voraussetzung für die weiteren, wahlweise zu installierenden Optionen.

- **Domino-Server (Option *BASE)**
  enthält Programme, Daten und Schablonendateien, die zum Ausführen des Domino-Servers notwendig sind. Diese Option ist Grundvoraussetzung für die weiteren Optionen und muss installiert werden.

- **AS/400-Integration (Option 1)**
  enthält AS/400-Programme und Objekte. Sie dienen zum einen der Synchronisation des AS/400-Verzeichnisses mit dem Domino-Verzeichnis und zum anderen der Kontrolle des Domino-Servers über die grafische Benutzeroberfläche (Operations Navigator). Für die Verzeichnissynchronisation ist weiterhin noch Option 6 (HiTest C API) erforderlich!

- **C API (Option 3)**
  ist notwendig für das Erstellen von C-Anwendungen in Notes, die auf der AS/400 ausgeführt werden.

- **C++ API (Option 4)**
  ist notwendig für das Erstellen und Ausführen von C++-Anwendungen auf einem Domino-Server.

4.2.2.0.3 Optionen unter Release 6

Die unter Release 4 und 5 zur Verfügung stehenden sieben Optionen wurden durch Wegfall bzw. Umgliederung im Release 6 zu zwei Optionsvarianten zusammengefasst:

- **Domino-Server (Option *BASE)**
  enthält Programme, Daten und Schablonendateien, die zum Ausführen des Domino-Servers notwendig sind sowie den SMTP-Support, DECS, den HTTP-Server sowie die Hilfe-Datenbanken. Diese Option ist Grundvoraussetzung für die weiteren Optionen und muss installiert werden.

- **C API (Option 1)**
  ist notwendig für das Erstellen von C-Anwendungen in Notes, die auf der iSeries ausgeführt werden.

Mit dem Release 6.0.3 und dem Release 6.5 steht die Multiversioning-Version zur Verfügung, mit der auf einer iSeries in einer Partition mehrere Domino-Release-Versionen parallel installiert werden können. Die einzelnen Domino-Releases werden dann auf der iSeries durch unterschiedliche Optionen differenziert:

Für Release 6.0.x lauten die Optionen:

Release	Option
6.0.3	13
6.0.4	14
6.0.5	15

Für Release 6.5.x lauten die Optionen:

Release	Option
6.5.0	10
6.5.1	11
6.5.2	12

4.2.2.0.4 Sprachversionen

Die Installation von länderspezifischen Versionen unterscheidet sich wesentlich von der Installation früherer Releases.

Standen bisher besondere landesspezifische Installationsverfahren (z.B. Deutsche Serverversion) zur Verfügung, so muss seit Release 6 zunächst immer die Englische Version installiert werden; anschließend kann man das jeweilige Language Pack zusätzlich installieren.

Diese Seite ist zur Zeit nicht belegt.

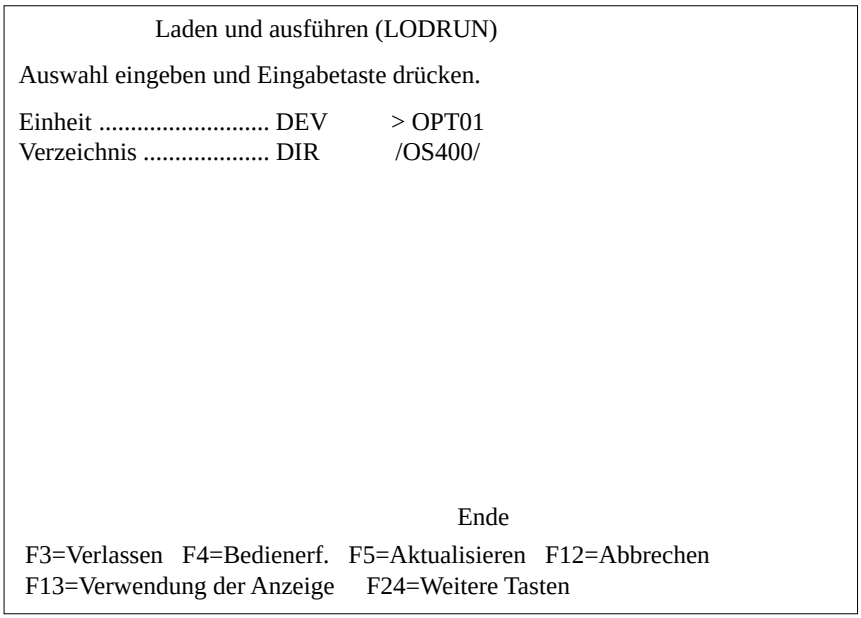
4.2.2.1 Installation der Domino-Software

Nachdem die Mindestanforderungen im Software- und Hardwarebereich geprüft sind und entschieden ist, welche Komponenten der Notes-Software installiert werden müssen, kann mit der Installation begonnen werden. Achten Sie aus lizenzrechtlichen Gründen darauf, dass pro installiertem Server eine entsprechende Lizenz vorhanden sein muss.

Die Software für die AS/400-Version von Lotus Domino wird auf einer gesonderten CD ausgeliefert. Verwenden Sie für die

Installation nur diese CD! Legen Sie diese CD in das Laufwerk der AS/400 ein.

Das Einspielen der Software wird mittels dem Befehl LODRUN gestartet. Der Befehl LODRUN erfordert 2 Parameter, nämlich die Laufwerksangabe (Parameter dev) und die Pfadangabe (Parameter dir). Drücken Sie nach der Eingabe von LODRUN die „F4“-Taste und Sie gelangen in den Prompt-Mode, in dem Sie die notwendige Parametrisierung durchführen können. Wählen Sie in dieser Anzeige zunächst die CD-Einheit aus (i.d.R OPT01). Drücken Sie nun die Eingabetaste, und ein weiterer Parameter, „Verzeichnis“, wird eingeblendet. Geben Sie hier das Verzeichnis an, in dem sich die Domino-für-AS/400-Software befindet.



Der Befehl LODRUN

Kennzeichnen Sie nun in der nächsten Maske all die Programmoptionen, die Sie auf Ihrem System installieren wollen.

```
                Lizenzprogramm Lotus Domino für AS/400 (5769LNT) installieren

Auswahl eingeben, Eingabetaste drücken.
  1=Installieren

          Produkt  Installiert
Option    Option   Status      Beschreibung
  1       *BASE    *NO         Domino-Server 4.6
  1       1        *NO         AS/400 Integration
  1       3        *NO         C API Release 4.5
  1       4        *NO         C++ API Release 4.1
  1       5        *NO         LotusScript Extension Toolkit
  1       6        *NO         HiTest C API Release 4.5
          7        *NO         Advanced Services




 F3=Verlassen   Eingabetaste—>Weiter

 (C) COPYRIGHT IBM CORP. 1980, 1998.
 (C) COPYRIGHT LOTUS DEVELOPMENT CORP. 1998.
 Option *BASE wird installiert ...
```

Die Installation der Domino-Software

Nach erneuten Drücken der Eingabetaste wird die Lotus-Domino-Software auf Ihrer AS/400 installiert.

Während der Installation der Domino-Software werden

- Programme und Dateien des AS/400-Domino-Servers in die Bibliothek QNOTES gespielt;
- Ressource-Dateien von AS/400-Domino im IFS (Integriertes File-System) gespeichert (/QIBM/PRODDATA/LOTUS/NOTES);
- Verknüpfungen zwischen QNOTES und dem IFS erstellt;
- das Benutzerprofil QNOTES angelegt (Dies ist ein internes Benutzerprofil, das für die Integration von Domino auf der AS/400 verwendet wird. Eine Anmeldung mit diesem Benutzer ist nicht möglich!).

Nach erfolgter Installationen prüfen Sie, ob Lotus Domino auf Ihrer AS/400 korrekt installiert worden ist. Gehen Sie dazu wie bei der Überprüfung der notwendigen Software mit dem Menü „LICPGM“ vor, oder verwenden Sie den Befehl zur Anzeige der Software-Ressourcen „DSPSFWRSC. Suchen Sie in beiden Fällen nach einem Eintrag 5769-LNT. Für jede von Ihnen bei der Installation ausgewählten Produktoption muss nun ein Eintrag vorhanden sein.

Softwareressourcen anzeigen
System: S44R3881

Ressour.	Option	eature	Beschreibung
5763XD1	*BASE	5050	Client Access/400 – Optimiert für Windows
5763XD1	*BASE	2929	Client Access/400 – Optimiert für Windows
5769LNT	***BASE**	**5050**	**Lotus Domino für AS/400**
5769LNT	*BASE	2929	Lotus Domino für AS/400
5769LNT	1	5050	AS/400 Integration
5769LNT	1	2929	AS/400 Integration
5769LNT	3	5050	C API
5769LNT	4	5050	C++ API
5769LNT	5	5050	LotusScript Extension ToolKit
5769LNT	**6**	**5050**	**HiTest C API**
5769PM1	*BASE	5050	IBM Performance Management/400
5769PM1	*BASE	2929	IBM Performance Management/400
5769PW1	*BASE	5050	Application Development ToolSet/400 – SEU
5769PW1	*BASE	2929	Application Development ToolSet/400 – SEU

Weitere ...

Eingabetaste —> Weiter

F3=Verlassen F11=Bibliotheken/Releases anzeigen F12=Abbrechen
F19=Marken anzeigen

Anzeige der Softwareressourcen

Der Eintrag 5769LNT mit der Option *BASE ist zweifach in der Anzeige vorhanden. Der Eintrag mit der Feature-Nummer 5050 enthält die sprachenunabhängigen Programme und Dateien, der Eintrag mit dem Feature-Code 2929 enthält die sprachenabhängigen Objekte (2929 = Deutsch).

4.2.2.2 Domino-Konfiguration

Wie bereits beschrieben, besteht zwischen der Behandlung der Installation des ersten Servers in einer Organisation und weiterer Server ein Unterschied. Im nachfolgenden Konfigurationsbeispiel wird davon ausgegangen, dass es sich um die Installation des ersten Servers handelt. Stellen Sie nochmals sicher, dass alle notwendigen Informationen für die Einrichtung des ersten Servers zur Hand sind. Diese Informationen, die identifizierend für den Domino-Server (und damit auch für alle zugehörigen Clients) sind, können später nicht mehr geändert werden! Während der Installation des ersten Servers wird:

- eine neue Domäne für den (die) Domino-Server erstellt
- das Netzwerk und die Anschlüsse aktiviert
- das Domino-Verzeichnis erstellt (NAMES.NSF)
- die Zertifizierer-ID für das Unternehmen erstellt (CERT.ID)
- die Server-ID (SERVER.ID) erstellt
- die Server-ID zugelassen
- die Administrator-ID erstellt
- ein Server-Dokument im Domino-Verzeichnis erstellt
- ein Mail-Verzeichnis erstellt

Beachten Sie, dass die Konfiguration des Domino-Servers im Normalfall interaktiv erfolgt. Dadurch kann eine Performance-Verschlechterung während des Konfigurationsvorganges eintreten.

Für die Konfiguration verwenden wir im nachfolgenden Beispiel eine 5250-Emulation. Geben Sie in die Befehlszeile den Befehl „CFGDOMSVR“ ein und drücken Sie die „F4“-Taste. Sie werden nun zur Eingabe des Server-Namens aufgefordert. Günstigstenfalls verwenden Sie den TCP/IP-Host-Namen Ihrer AS/400 als Server-Namen. Sollten Sie einen anderen Namen verwenden wollen, so denken Sie daran, den TCP/IP-Host-Eintrag anzugeben! Als Option geben Sie „*FIRST“ an. Dies identifiziert die Installation des ersten Servers.

```
                Domino-Server konfigurieren (CFGDOMSVR)

Auswahl eingeben und Eingabetaste drücken.

Server-Name ..... ZEBIS1


Option ..... *FIRST        *FIRST, *ADD, *REMOVE




                                                Ende
F3=Verlassen  F4=Bedienerf.  F5=Aktualisieren  F12=Abbrechen
F13=Verwendung der Anzeige    F24=Weitere Tasten
```

Der Befehl CFGDOMSVR

Im Feld „Option“ haben Sie neben der Angabe *FIRST und *ADD (für zusätzliche Server) noch die Möglichkeit, einen bereits installierten Server mit dem Eintrag „*REMOVE“ zu entfernen. Achtung! Bevor Sie diese Option auswählen, beachten Sie bitte, dass nicht nur der ausgewählte Domino-Server gelöscht wird, sondern darüber hinaus auch alle Dateien und Anwendungen, die diesem Server zugeordnet sind, gelöscht werden. Nach der Eingabe „*FIRST“ bestätigen Sie nun mit der Eingabetaste die Auswahl.

Anschließend erscheint nun eine erweiterte Anzeige. Geben Sie in den Feldern „Zulassungsstellen-ID“; „Administrator-ID“ und „Server-ID“ als Unterlassungswert „*GEN“ ein. Durch diesen Eintrag erstellt der Konfigurationsprozess die erforderlichen ID-Dateien selbständig in das Verzeichnis, dass Sie als Datenverzeichnis angeben müssen. Als weitere Angaben sind zu vorzunehmen:

- Verzeichnis Data z.B. /notes/data
- Unternehmensname
  Organisationsname
- Administratorname und Kennwort
- Mindestkennwortlänge des Administrators
  max. 31 Zeichen
- Zeitzone
- Verwendung der Sommerzeit
  In Deutschland *YES eingeben.

- Domänenname

  *ORG -> der Domänenname des Domino-Servers ist identisch mit dem Namen der Organisation. Achten Sie darauf, dass kein bereits in Ihrem Umfeld existierender Domänenname verwendet wird!

- Netzwerkname

  Als Default-Wert ist „NETWORK1“ eingetragen. Existiert bereits ein Domino-Netzwerk, so ersetzen Sie den Default-Wert durch den Namen Ihres Netzwerkes (zu finden im Domino-Verzeichnis unter der Rubrik „eingetragene Server“). Existiert noch kein Netzwerk, so empfehle ich, einen sprechenderen Namen als den Default-Wert einzutragen.

- die Landes-ID

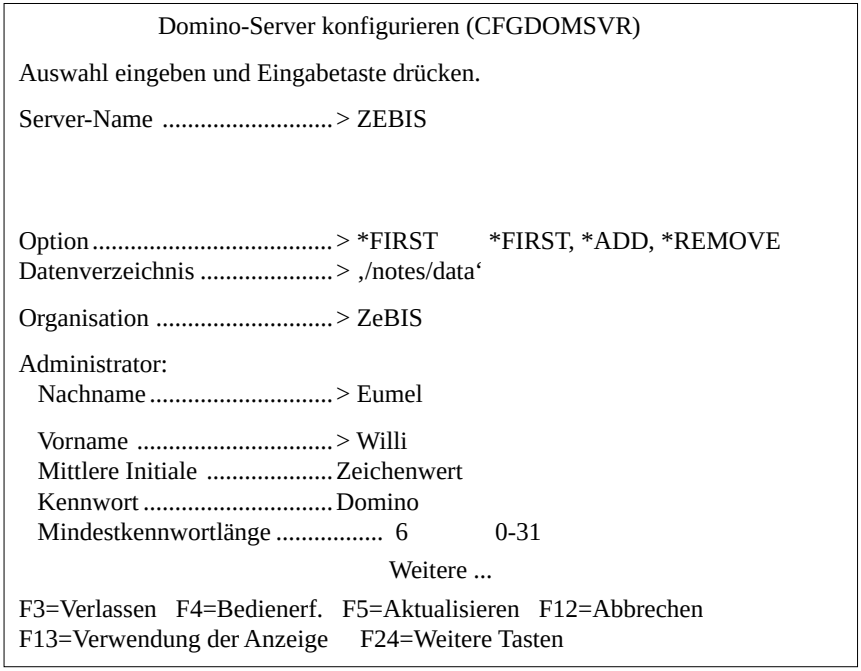
  wird der Zulassungs-ID des Domino-Servers hinzugefügt; DE=Deutschland.

- Eintrag, ob die Replikationsergebnisse in die LOG.NSF eingetragen werden sollen

- Eintrag, ob Client-Sitzungsergebnisse in der LOG.NSF eingetragen werden sollen

- Angabe, ob ein Web-Browser-Feature mitkonfiguriert werden soll.

  Ermöglicht den Zugriff von Web-Browsern auf den Domino-Server.



Der Befehl CFGDOMSVR (erweiterte Anzeige)

Blättern Sie mit der „Bild ab“-Taste nun auf die nächste Seite.

Domino-Server konfigurieren (CFGDOMSVR)

Auswahl eingeben und Eingabetaste drücken.

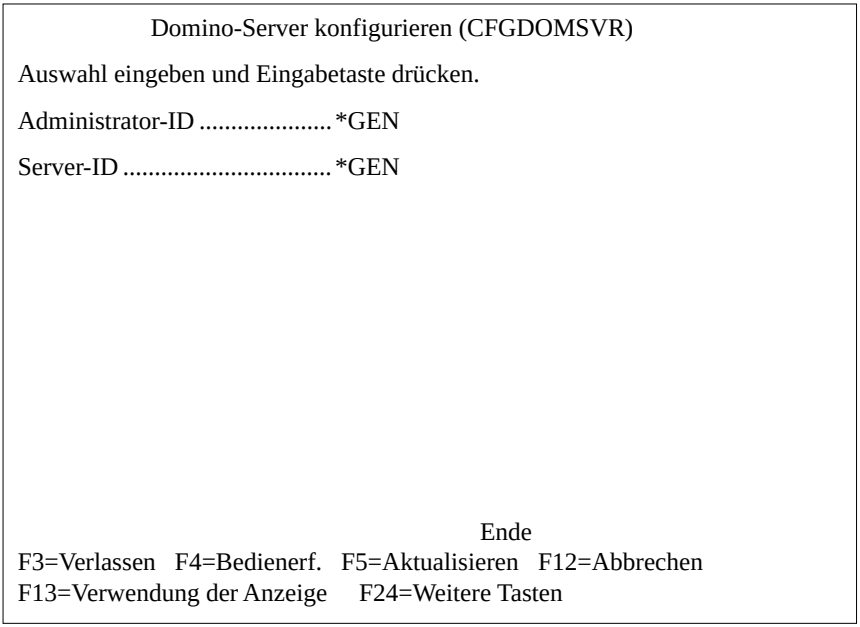
Zeitzone	> CET	GMT,EST,CST,MST,PST,CET ...
Sommerzeit	*YES	*YES, *NO
Domänenname	*ORG	
Netzwerkname	NETWORK1	
Landes-ID	DE	
Replikationsereignisse prot	*YES	*YES, *NO
Client-Sitzungsereign. prot	*YES	*YES, *NO
Konfiguration ersetzen	*YES	*YES, *NO
Web Browser	*http	*NONE, *HTTP
News Reader	*NONE	*NONE, *NNTP
Internet Mail Packages	*NONE	*NONE, *ALL, *IMAP, *LDAP...
+ für weitere Werte		
Advanced Services	*NONE	*NONE, *ALL, *PARTITION...
+ für weitere Werte		
Zulassungs-ID	*GEN	

Weitere ...

F3=Verlassen F4=Bedienerf. F5=Aktualisieren F12=Abbrechen
F13=Verwendung der Anzeige F24=Weitere Tasten

Der Befehl CFGDOMSVR (erweiterte Anzeige)

Nach erneutem Betätigen der „Bild ab“-Taste gelangen Sie auf die letzte Seite der Domino-Server-Konfiguration.



Der Befehl CFGDOMSVR (erweiterte Anzeige)

Drücken Sie nun die Eingabetaste, wird Ihr Domino-Server konfiguriert.

Während der Installation sehen Sie auf dem Bildschirm in einer Statusanzeige, welcher Befehl gerade ausgeführt wird.

```
/ZeBIS/DE wird registriert...
ID für /ZeBIS/DE wird erstellt.  Dieser Vorgang dauert 1-3 Minuten...
Registrierung für /ZeBIS/DE war erfolgreich.
ID für Willi Eumel/ZeBIS/DE wird erstellt.  Dieser Vorgang dauert 1-3 Minuten
...
Willi Eumel/ZeBIS/DE wird zugelassen...
Zulassung von Willi Eumel/ZeBIS/DE abgeschlossen...









===>

F3=Verlassen  F4=Dateiende  F6=Drucken  F9=Auffinden  F17=Anfang
F18=Ende  F19=Links  F20=Rechts  F21=Benutzerfenster
```

Status der Konfiguration I

```
ID für Willi Eumel/ZeBIS/DE wird erstellt.  Dieser Vorgang dauert 1-3 Minuten
...
Willi Eumel/ZeBIS/DE wird zugelassen...
Zulassung von Willi Eumel/ZeBIS/DE abgeschlossen...
/ZeBIS/DE wird registriert...
/ZeBIS/DE wird in das Namen- und Addressbuch aufgenommen...
Registrierung für /ZeBIS/DE war erfolgreich.
ZEBIS wird registriert...
ID für ZEBIS/ZeBIS/DE wird erstellt.  Dieser Vorgang dauert 1-3 Minuten...
ZEBIS/ZeBIS/DE wird zugelassen...
Zulassung von ZEBIS/ZeBIS/DE abgeschlossen...
ZEBIS/ZeBIS/DE wird in das Namen- und Addressbuch aufgenommen...
Registrierung für ZEBIS/ZeBIS/DE war erfolgreich.
Willi Eumel wird registriert...
Mail-Datei für Willi Eumel/ZeBIS/DE wird erstellt...
Willi Eumel/ZeBIS/DE wird in das Namen- und Addressbuch aufgenommen...
Registrierung für Willi Eumel/ZeBIS/DE war erfolgreich.
Die Eingabetaste drücken, um die Datenstationssitzung zu beenden.

===>

F3=Verlassen  F4=Dateiende  F6=Drucken  F9=Auffinden  F17=Anfang
F18=Ende    F19=Links    F20=Rechts    F21=Benutzerfenster
```

Status der Konfiguration II

Die Konfiguration kann durchaus 30 Minuten und mehr in Anspruch nehmen. Dieser Wert variiert je nach AS/400-Modell.

Sobald die Anzeige besagt, dass der Konfigurationsvorgang abgeschlossen ist, drücken Sie die Eingabetaste und prüfen anschließend die Konfiguration

```
MAIN                    IBM AS/400 Hauptmenü
                                        System:  S44R3881
Auswahlmöglichkeiten:

    1. Benutzeraufgaben
    2. Büroaufgaben
    3. Allgemeine Systemaufgaben
    4. Dateien, Bibliotheken und Ordner
    5. Programmierung
    6. Datenfernverarbeitung
    7. System definieren oder ändern
    8. Problembehandlung
    9. Menü anzeigen
   10. Unterstützende Informationen - Auswahlmöglichkeiten
   11. Client Access/400-Aufgaben

   90. Abmelden

Auswahl oder Befehl
===>

F3=Verlassen  F4=Bedienerführung  F9=Auffinden  F12=Abbrechen
F13=Unterstützende Informationen  F23=Anfangsmenü festlegen
Befehl CFGDOMSVR erfolgreich beendet.
```

CFGDOMSVR endet erfolgreich

4.2.2.3 Abschluss der Domino-Konfiguration

Um die Konfiguration des AS/400-Domino-Servers abschließend zu überprüfen, gehen Sie wie folgt vor: Geben Sie in der Befehlszeile den Befehl „STRDOMSVR“ gefolgt von dem von Ihnen vergebenen Server-Namen ein. Mit diesem Befehl wird der Domino-Server auf der AS/400 gestartet.

```
MAIN                        IBM AS/400 Hauptmenü
                                          System:  S44R3881
Auswahlmöglichkeiten:

    1. Benutzeraufgaben
    2. Büroaufgaben
    3. Allgemeine Systemaufgaben
    4. Dateien, Bibliotheken und Ordner
    5. Programmierung
    6. Datenfernverarbeitung
    7. System definieren oder ändern
    8. Problembehandlung
    9. Menü anzeigen
   10. Unterstützende Informationen – Auswahlmöglichkeiten
   11. Client Access/400-Aufgaben

   90. Abmelden

Auswahl oder Befehl
===> strdomsvr ZEBIS

F3=Verlassen  F4=Bedienerführung  F9=Auffinden  F12=Abbrechen
F13=Unterstützende Informationen  F23=Anfangsmenü festlegen
Domino-Server ZEBIS in Subsystem DOMINO01 wird gestartet.
```

Starten des Domino-Servers STRDOMSVR

```
                Mit aktiven Jobs arbeiten            S44R3881
                                          19.12.99  16:31:25
 CPU %:  21,7    Abgelaufene Zeit:  00:33:35    Aktive Jobs:  110

Auswahl eingeben und Eingabetaste drücken.
  2=Ändern  3=Anhalten  4=Beenden  5=Arbeiten mit    6=Freigeben
  7=Nachricht anzeigen  8=Mit Spool-Dateien arbeiten  13=Unterbrechen

Ausw. Subsystem/Job  Benutzer   Art   CPU %  Funktion              Status
  DOMINO01           QSYS       SBS   0,0    DEQW
  ADMINP             QNOTES     BCI   2,7    SELW
  AMGR               QNOTES     BCI   2,4    SELW
  AMGR               QNOTES     BCI   0,7    DEQW
  CALCONN            QNOTES     BCI   0,5    DEQW
  HTTP               QNOTES     BCI   3,1    SELW
  QNNINSTS           QNOTES     BCH   0,0    PGM-QNNINSTS  EVTW
  REPLICA            QNOTES     BCI   0,2    SELW
  ROUTER             QNOTES     BCI   0,8    SELW
                                      Weitere ...
Parameter oder Befehl
===>
F3=Verlassen  F5=Aktualisieren  F10=Neubeginn  F11=Aufgelaufene Daten
F12=Abbrechen  F23=Weitere Angaben  F24=Weitere Tasten
```

Mit aktiven Jobs arbeiten (WRKACTJOB)

Unter dem Subsystem DOMINOxx (xx = fortlaufende Nummerierung der Domino-Server auf der AS/400, für den ersten Server also „DOMINO01“) werden alle derzeit aktiven Tasks aufgelistet.

4.2.2.4 Domino-Konfiguration mit iSeries Navigator

Nachdem die Installation des Domino-Server-Codes erfolgt ist, muss der Server konfiguriert werden.

Die Konfiguration von Domino auf iSeries kann über

- iSeries Navigator,
- EZ Setup (seit Release 5.0.8),
- Domino Server Setup Wizard (domwzd.exe) und
- OS/400-Befehl CFGDOMSVR

erfolgen.

Alle diese Konfigurationsmethoden können auch zur Verwaltung von bereits konfigurierten Domino-Servern verwendet werden.

Wie bereits beschrieben, besteht zwischen der Behandlung der Installation des ersten Servers in einer Organisation und weiterer Server ein Unterschied. Im nachfolgenden Konfigurationsbeispiel wird davon ausgegangen, dass es sich um die Installation des ersten Servers handelt. Stellen Sie nochmals sicher, dass alle notwendigen Informationen für die Einrichtung des ersten Servers zur Hand sind. Diese Informationen, die identifizierend für den Domino-Server (und damit auch für alle zugehörigen Clients) sind, können später nicht mehr oder nur unter großem Aufwand geändert werden! Während der Installation des ersten Servers wird:

- eine neue Domäne für den (die) Domino-Server erstellt,
- das Netzwerk und die Anschlüsse aktiviert,
- das Domino-Verzeichnis erstellt (NAMES.NSF),

- die Zertifizierer-ID für das Unternehmen erstellt (CERT.ID),
- die Server-ID (SERVER.ID) erstellt,
- die Server-ID zugelassen,
- die Administrator-ID erstellt,
- ein Server-Dokument im Domino-Verzeichnis erstellt,
- ein Mail-Verzeichnis erstellt.

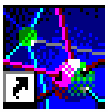
Nachfolgend wird an einem Beispiel die Neu-Konfiguration eines Domino-Servers, Release 6, unter Verwendung des iSeries Navigators demonstriert.

4.2.2.4.1 Installation des iSeries Navigator Plug-In

Voraussetzung für die Konfiguration und spätere Verwaltung mittels des iSeries Navigators ist das Domino Plug-In, das nicht im Rahmen der Grundinstallation des iSeries Navigators eingerichtet wird.

Sollte das Plug-In noch nicht installiert worden sein, müssen die nächsten Schritte erst ausgeführt werden. Ist das Domino Plug-In bereits installiert worden, kann der folgende Abschnitt übersprungen werden und direkt mit Abschnitt 4.2.2.5.2 weitergearbeitet werden.

Die Installation des Plug-Ins kann über den iSeries Navigator oder über die “Selektive Installation” von iSeries Access erfolgen:

IBM iSeries Access für Windows 

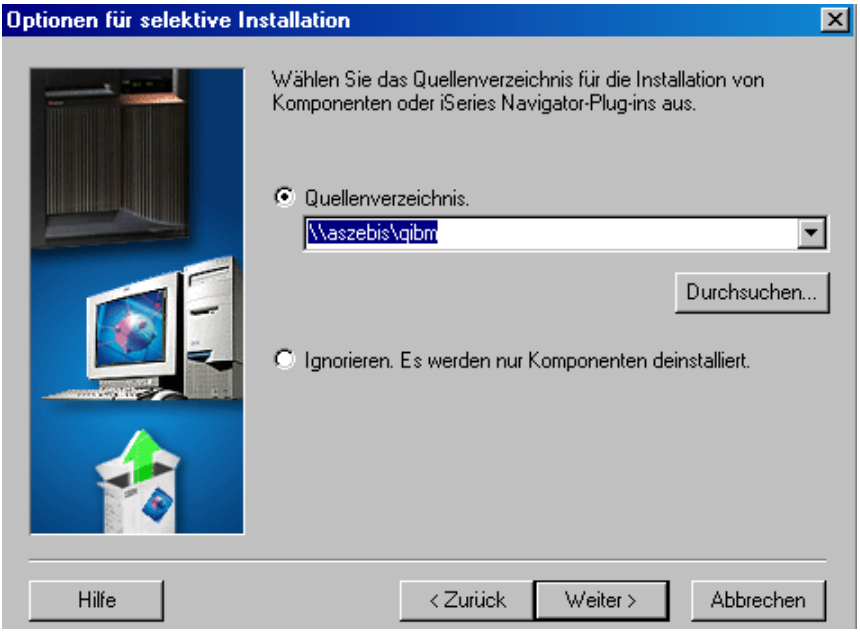
In der Programmgruppe des iSeries Access befindet sich auch die Gruppe für die „Selektive Installation“.

Selektive Installation

Nach Auswahl der „Selektiven Installation“ wird zunächst ein Hinweisfenster eingeblendet:

Komponenten hinzufügen

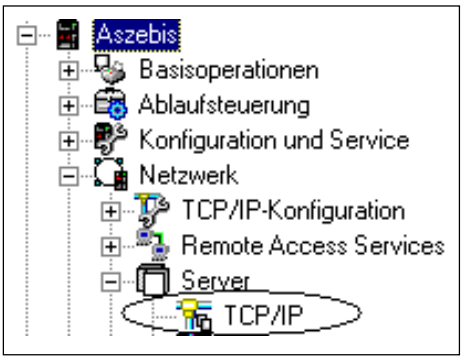
Die „Selektive Installation“ beinhaltet zugleich auch die Möglichkeit, bereits installierte Komponenten von dem PC zu entfernen. Da nun aber ein zusätzliches Feature installiert werden soll, wird in dem Eingabebereich das Quellverzeichnis in Form von \\NetServerName\QIBM angegeben.



Quellverzeichnis auswählen

Seit OS/400, Release V5R2M0 wird über NetServer auf die Verzeichnisse der iSeries zugegriffen. Sollte ein Fehler bei der Eingabe des Pfades auftreten, ist zu prüfen, ob der NetServer gestartet ist.

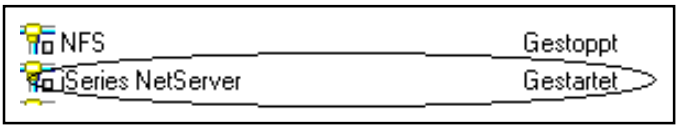
Dazu wird der iSeries Navigator gestartet und unter dem zu verwaltenden iSeries System der Ordner „Netzwerk“ geöffnet. Dort muss der Eintrag „Server“ geöffnet werden.



NetServer

Danach wird der Inhalt des Ordners „TCP/IP“ durch einen Doppelklick im rechten Bereich des Bildschirms aufgelistet.

Hier befindet sich auch der Eintrag für den NetServer. Dieser sollte den Status „Gestartet“ haben.



NetServer gestartet

Steht der Status auf „gestoppt“, kann der NetServer mit der rechten Maustaste gestartet werden.

NetServer starten

Alternativ kann der NetServer auch mit dem OS/400-Befehl “STRTCPSVR *NETSVR” gestartet werden.

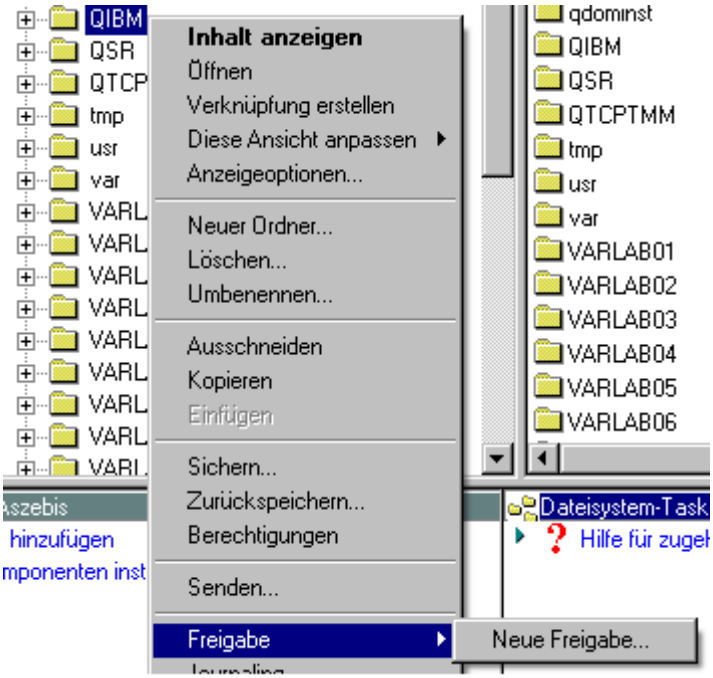
Um auf den NetServer zugreifen zu können, muss eine entsprechende Freigabe erfolgen. Diese kann ebenfalls über den iSeries Navigator erfolgen:

Im iSeries Navigator ist dazu der Eintrag „Dateisysteme“ zu öffnen. Darin befindet sich „Integrated File System“, in welchem wiederum das Verzeichnis „Root“ zu finden ist. Nach einem Klick auf „Root“ erscheint dessen Inhalt. Hier muss der Eintrag „QIBM“ gefunden werden.

QIBM freigegeben?

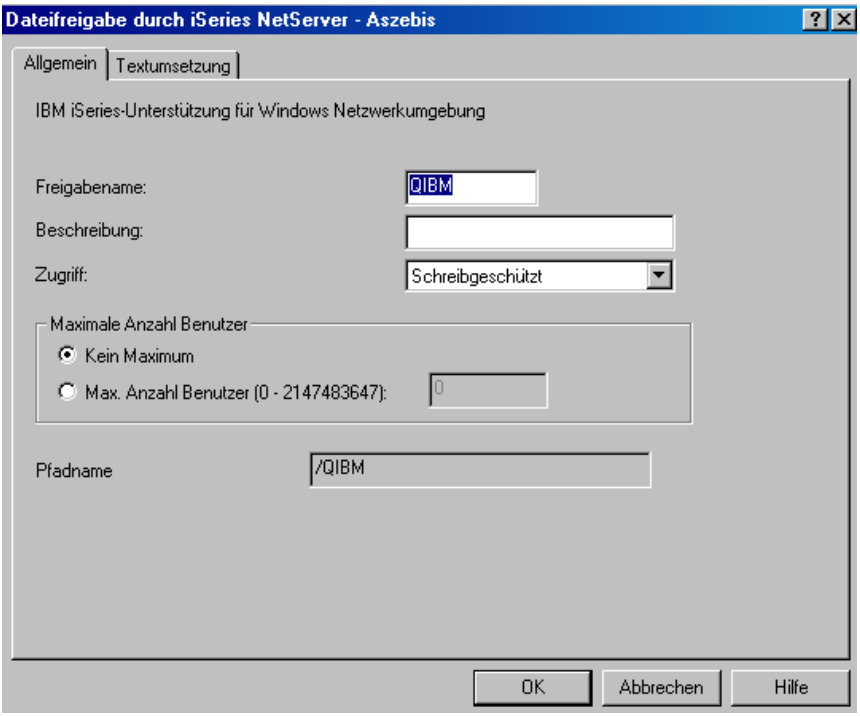
Ist links neben dem Eintrag „QIBM“ eine symbolische blaue kleine Hand zu sehen, dann ist eine Freigabe auf das Verzeichnis bereits erfolgt. Wird dieses Handsymbol nicht dargestellt, dann ist zunächst noch eine Freigabe erforderlich.

Diese Freigabe erfolgt nach einem Klicken mit der rechten Maustaste auf dem Eintrag „QIBM“. Dann wird der Eintrag „Freigabe“ markiert und mit „Neue Freigabe“ das Verzeichnis „QIBM“ freigegeben.



QIBM freigeben

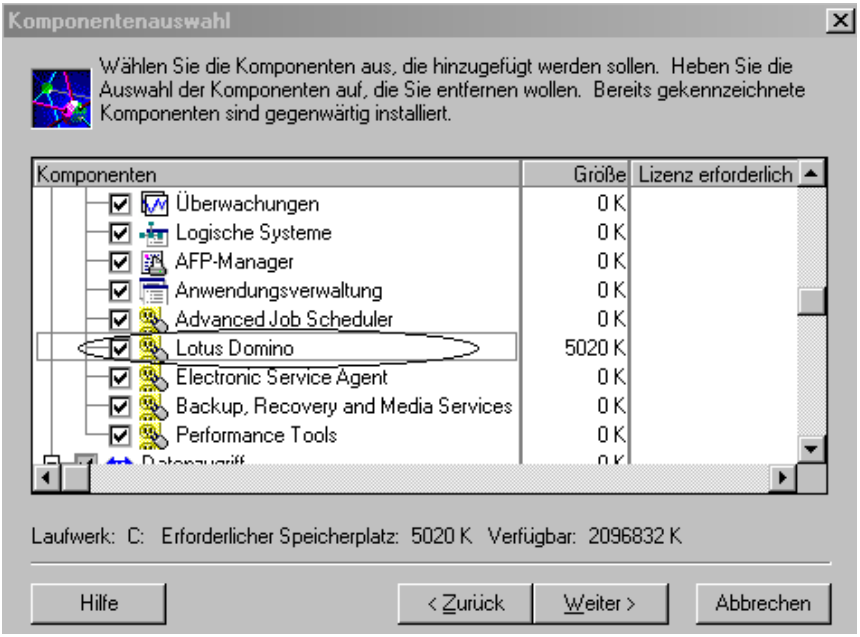
Zwar kann für die Freigabe ein Name gewählt werden, es empfiehlt sich aber die Übernahme der Voreinstellungen – ergänzt durch eine entsprechende Beschreibung in dem dafür vorgesehenen Feld. Mit einem Klick auf „OK“ ist die Freigabe erfolgt.



QIBM Freigabename

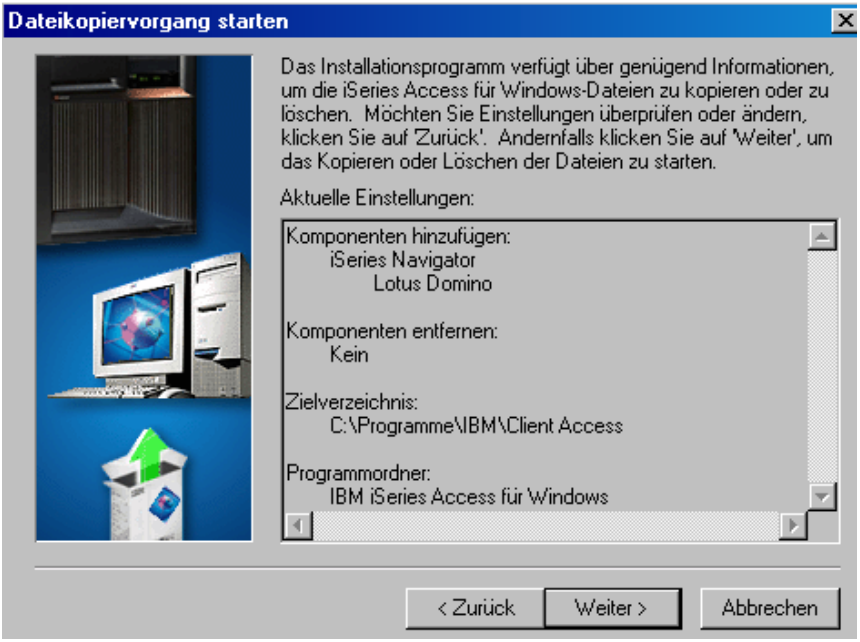
Danach sollte dann das Quellverzeichnis \\NetServerName\QIBM für die weitere Installation zugeordnet werden können.

Nun erscheint eine Auflistung aller bereits installierten Komponenten des iSeries Navigators. Der Eintrag „Lotus Domino“ wird nun mit der rechten Maustaste markiert und für die Installation ausgewählt.



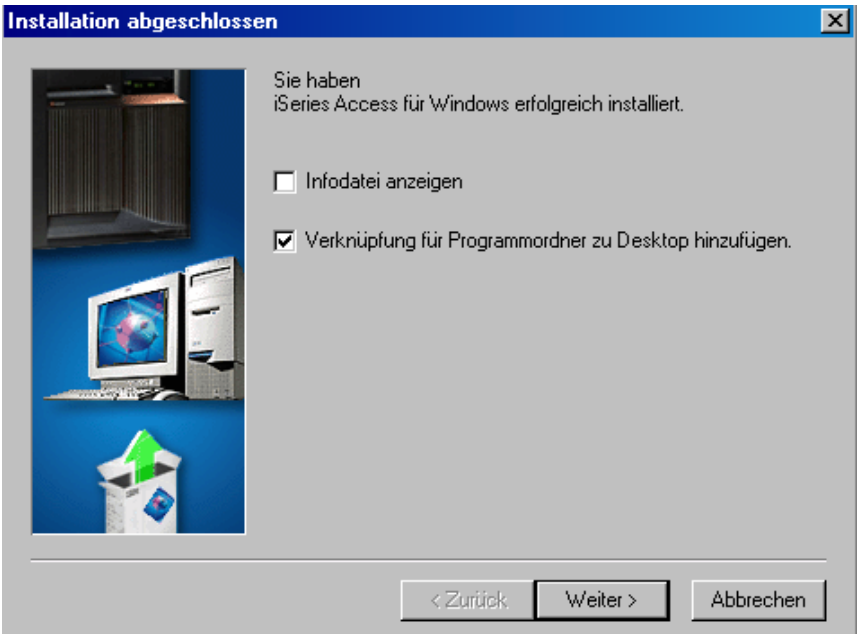
Komponentenauswahl

Nach einem Klick auf die Schaltfläche „Weiter“ gelangt man in die nächste Anzeige, die eine reine Information über die nun anstehende Installation darstellt.



Kopiervorgang starten

Ein weiterer Klick auf „Weiter“ startet nun die Installation, nach deren erfolgreichem Ende die Abschlussanzeige erscheinen sollte.



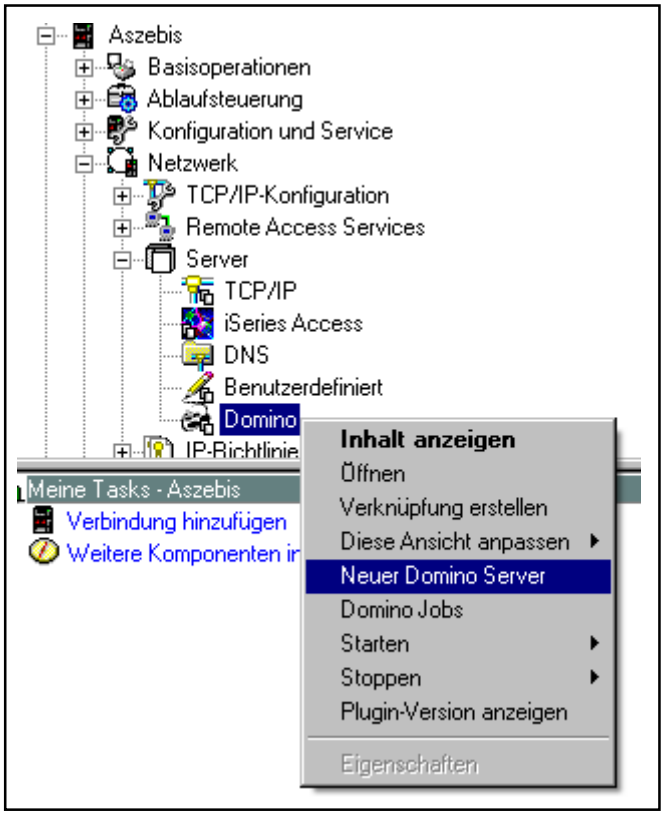
Installationsabschluss

Mit diesen Schritten sind die Voraussetzungen geschaffen, Domino über den iSeries Navigator konfigurieren zu können.

4.2.2.4.2 Konfigurationsausführung

Die eigentliche Konfiguration eines Domino-Servers auf iSeries kann nun über den iSeries Navigator gestartet werden.

Dazu wird das zu verwaltende iSeries-System ausgewählt und unter dem Pfad „Netzwerk _ Server“ der Eintrag „Domino“ mit der rechten Maustaste ausgewählt.

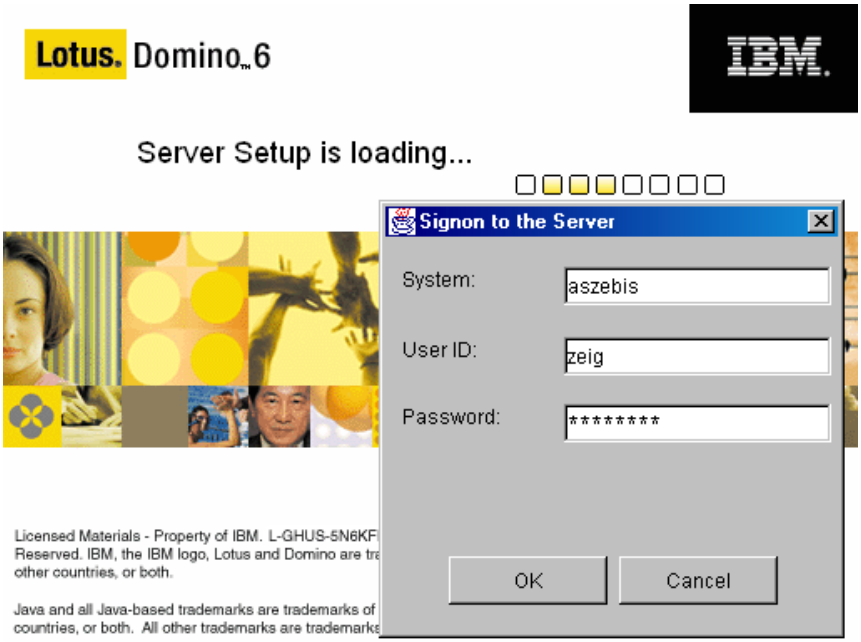


Neuer Domino Server

Neben der Verwaltung bestehender Server, dem Starten und Stoppen von Domino-Servern, kann auch ein neuer Server installiert werden.

Die Version des Plug-Ins enthält den Release-Stand der Domino Installation, denn das Plug-In stammt von der Domino-CD. Achten Sie darauf, bei Server-Upgrades auch das Plug-In anzupassen!

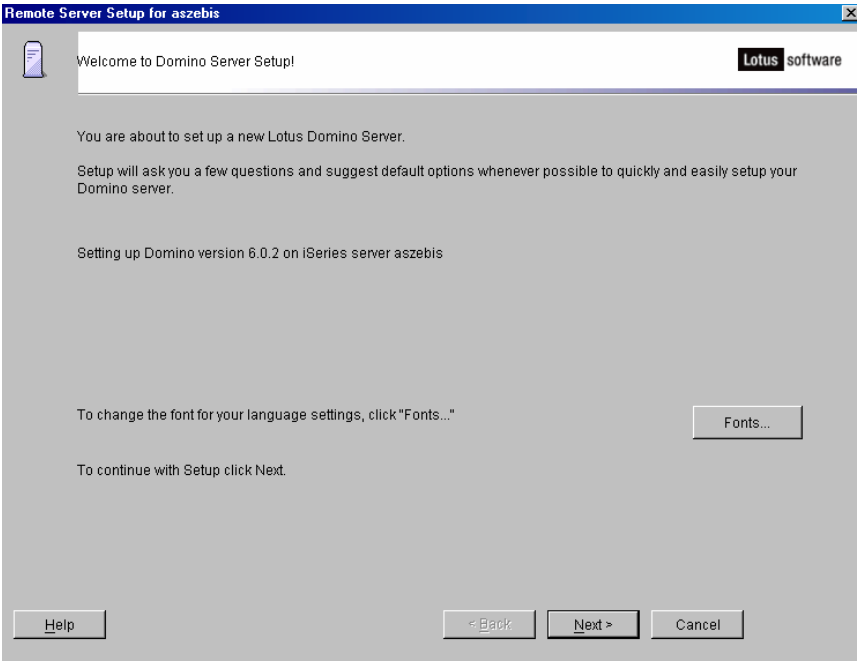
Für die Neukonfiguration eines Domino-Servers ist die Anmeldung auf der iSeries erforderlich. Diese wird durch ein Java-Fenster initialisiert. Hier ist keine Case-Sensitive-Eingabe notwendig. Der für die Installation ausgewählte Benutzer sollte mindestens über die Berechtigungen *ALLOBJ, *SECADM, *JOBCTL und *IOSYSCFG verfügen.



Signon

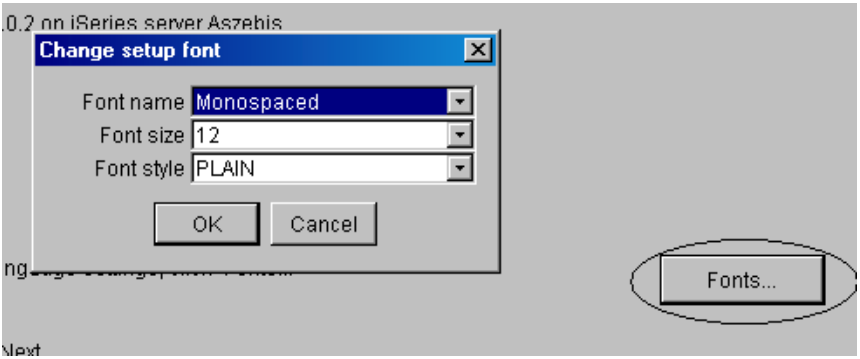
Der in allen grafischen Installationsmethoden ähnliche Wizard führt nun durch die Konfiguration. Dabei steht eine Bedienerhilfe mit Erklärungen über die Bedeutung der zu treffenden Auswahlen durch einen Klick auf die Schaltfläche „Help“ bzw. „Hilfe“ zur Verfügung.

Die Konfiguration kann jederzeit durch „Cancel“ abgebrochen werden. Durch die Schaltfläche „Back“ erfolgt der Sprung auf die vorgelagerte Maske.



Remote Setup Konfiguration

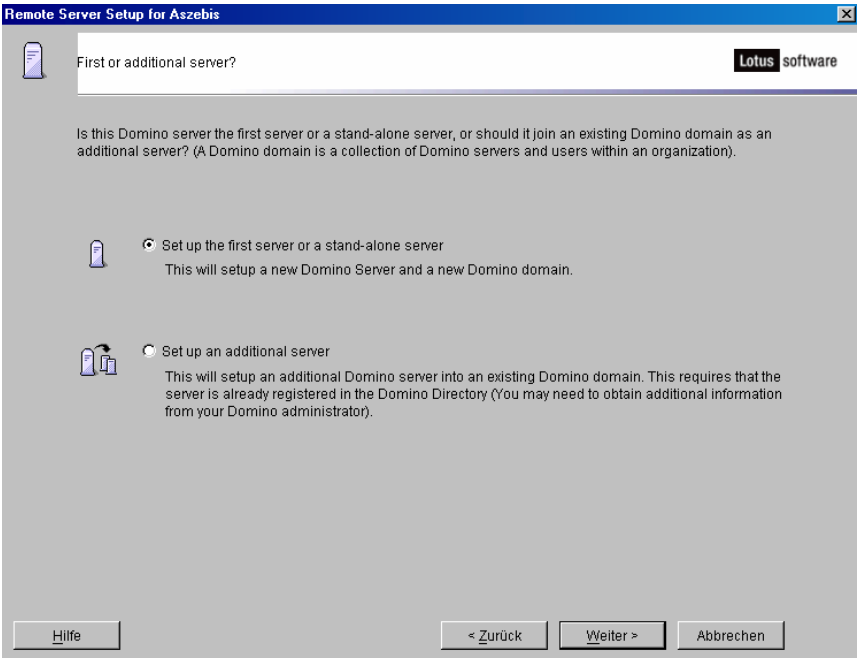
Sprachenabhängig können mit Auswahl der Schaltfläche „Fonts“ die Einstellungen angepasst werden.



Länderspezifische Fonts

Die Beschreibung der Unterschiede zwischen der Installation des ersten Domino-Servers und weiterer Domino-Server in einer Domäne ist bereits in Kapitel 4.2.2 erfolgt.

Nachfolgendes Beispiel zeigt die Konfiguration eines ersten Servers in einer Domäne. Zwar gibt es keine sprachindividuellen oder übersetzte Installationsmethoden, aber die Schaltflächen haben hier offenbar ihre eigene Intelligenz, denn diese erscheinen nun in der jeweiligen Landessprache.



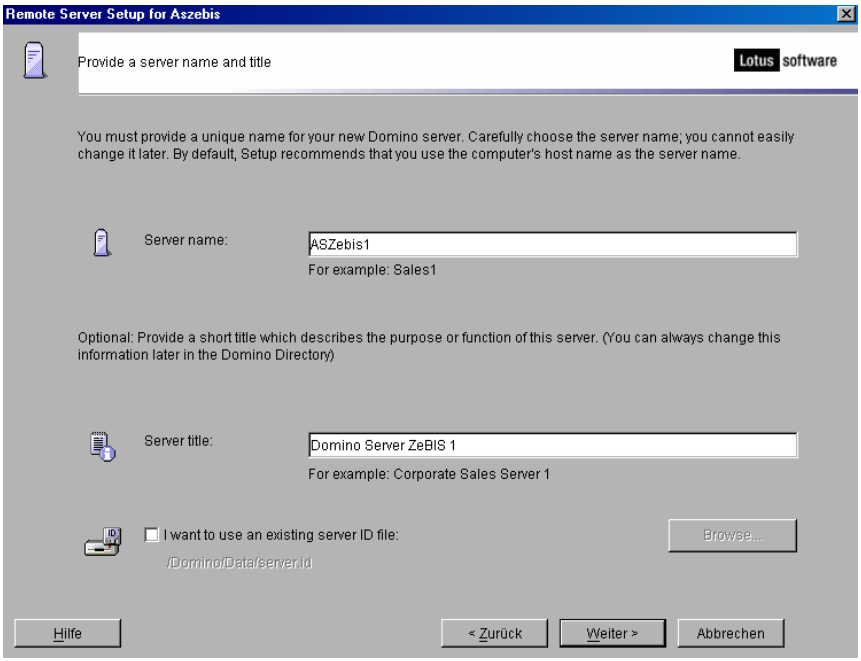
Erster oder zusätzlicher Server

Nun ist der Server-Name zu vergeben. Oftmals wird hier der iSeries-Name verwendet, wodurch Anpassungen im TCP/IP der iSeries nicht nötig sind. Ist der Server Name einmal festgelegt und definiert, lassen sich Änderungen nur sehr schwer vornehmen.

Selbstverständlich kann auch ein anderer Name als der Name der iSeries verwendet werden. Dazu müssen dann einige Änderungen an den TCP/IP-Definitionen vorgenommen werden.

In unserem Beispiel bekommt der Domino-Server denselben Namen wie die iSeries.

Wurde bereits durch eine frühere Konfiguration eine Server-ID erstellt und soll im Zuge der Konfiguration keine neue Server-ID generiert werden, dann kann die Auswahl „I want to use an existing server ID file“ ausgewählt werden. Existiert keine Server-ID, dann wird diese im Laufe der Konfiguration erstellt.

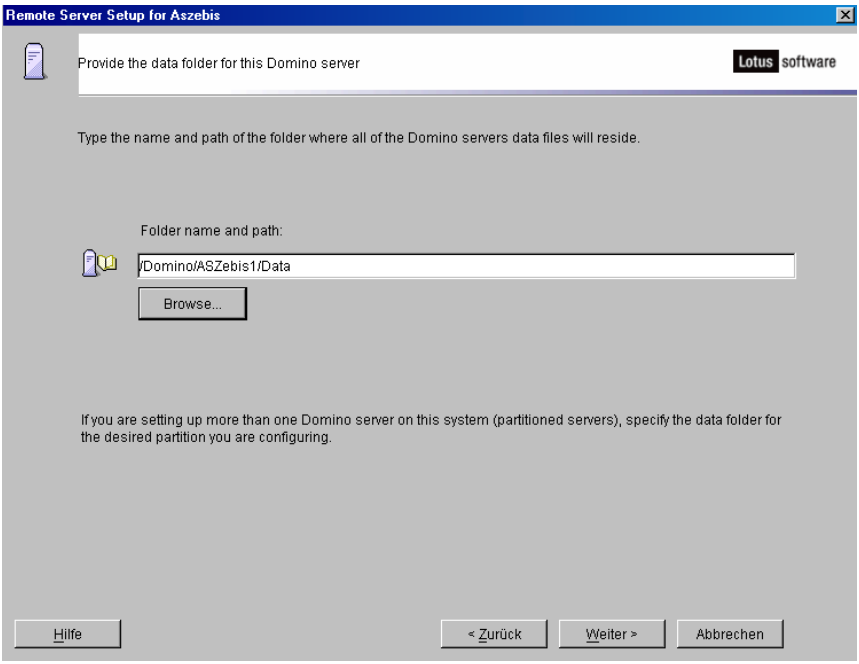


Servername

Die Daten von Domino werden innerhalb des OS/400 Integrated File System (IFS) abgelegt. Der Standardpfad für die Speicherung der Domino-Daten wird mit „/Domino/*dominoservername*/Data“ voreingestellt. Der Installationspfad kann aber auch abgeändert werden.

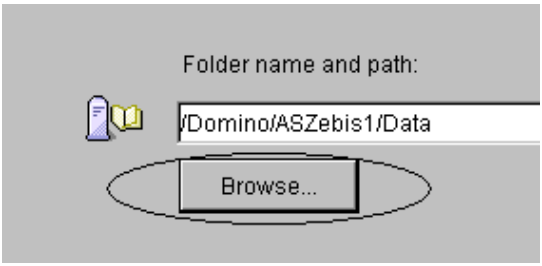
Sollen auf einer iSeries mehrere Domino-Server aufgesetzt werden, dann muss der Installationspfad angepasst werden, denn für jeden Server muss ein eigener Pfad angegeben werden.

In der Praxis hat sich hier die Angabe des Domino-Server-Namens bewährt.

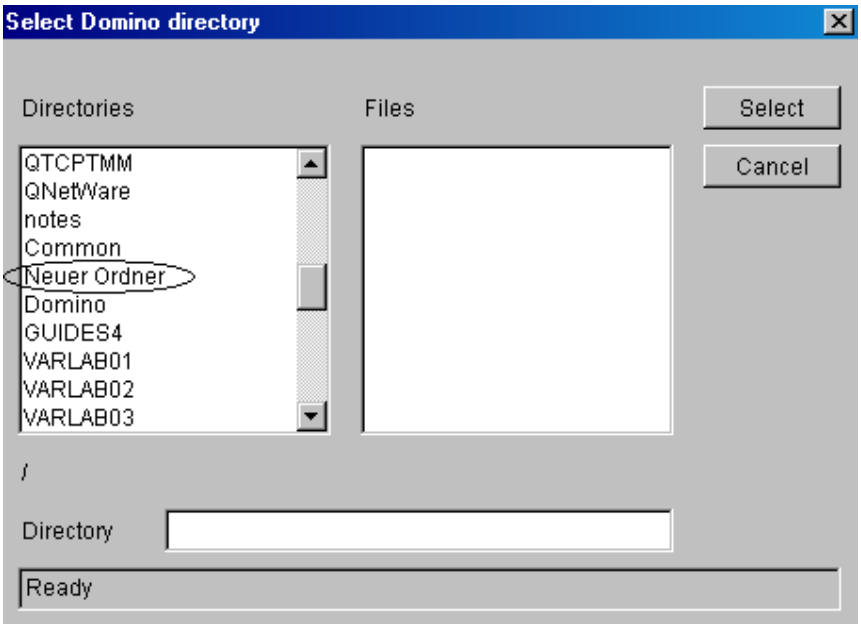


Pfadangabe

Soll ein anderer Pfad innerhalb des IFS verwendet werden, kann die Voreinstellung überschrieben werden. Dabei kann auch ein noch nicht existierendes Verzeichnis angegeben werden, das dann automatisch erstellt wird.



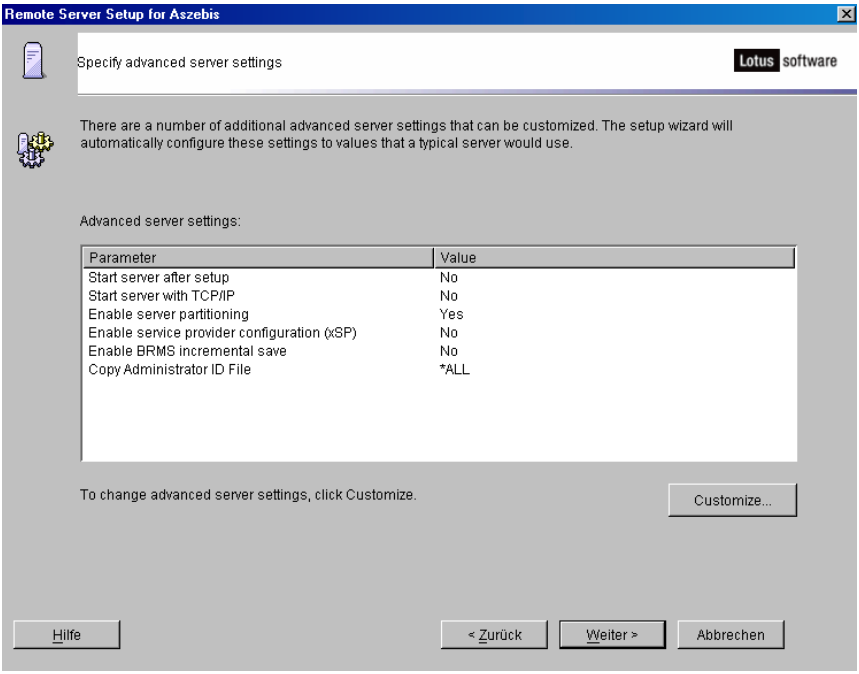
Browse



Modifizierter Pfad

Im nächsten Window können neben den Standard-Installationsvorgaben zusätzliche Optionen konfiguriert werden. So kann unter anderem angegeben werden, dass der Domino-Server automatisch nach einem Setup oder während eines STRTCP mitgestartet werden soll.

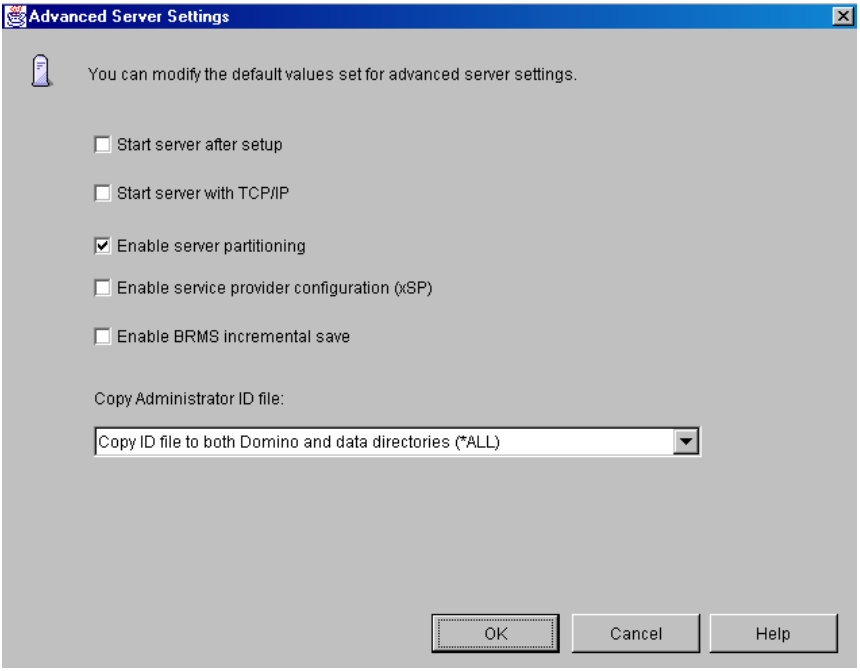
Wird auf der iSeries BRMS (Backup and Recovery Media Systems – Lizenzprogramm 5722-BR1) eingesetzt, kann mit diesem Tool eine inkrementelle Datensicherung der Domino-Daten durchgeführt werden. Ist dies gewünscht, sollte der entsprechende Eintrag ausgewählt werden.



Erweiterte Server-Einstellungen

Eine Anpassung der voreingestellten Default-Werte ist über die Schaltfläche „Customize…“ möglich.

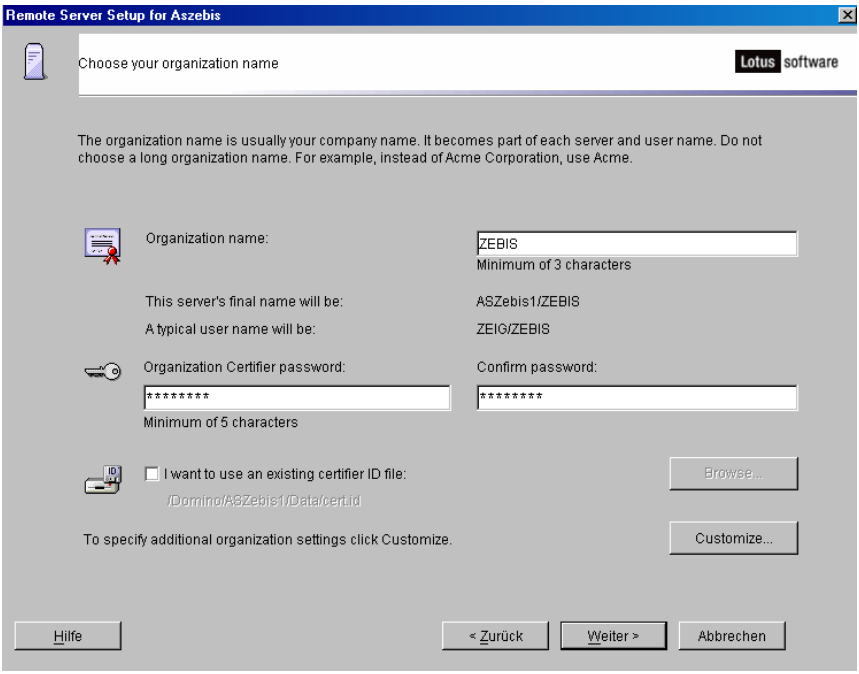
Anpassungen



Erweiterte Einstellungen

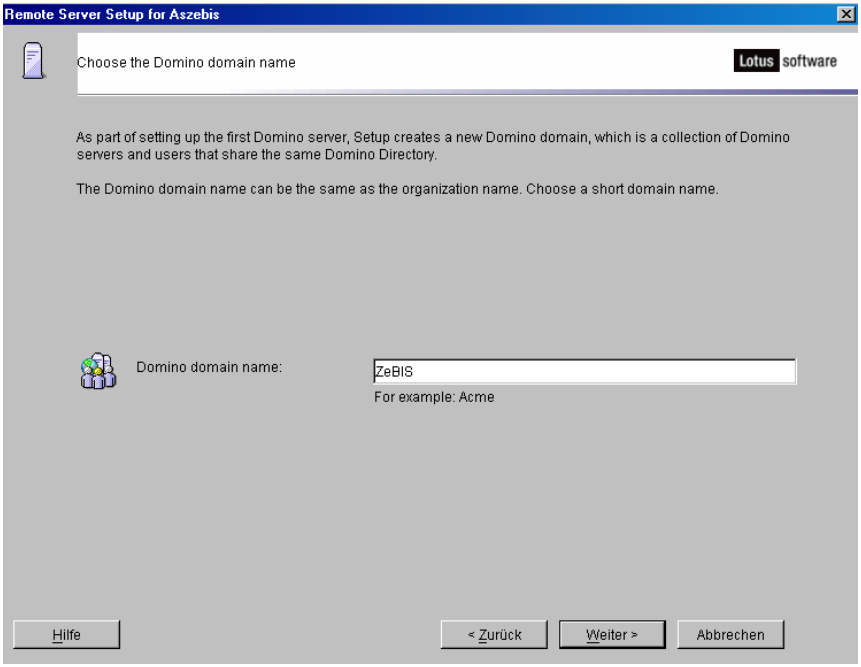
Die nun folgenden Einstellungen definieren den Namen Ihrer Organisation. Zudem ist das Certifier-Kennwort zweifach einzugeben. Entgegen der iSeries-Kennworteingabe wird hier zwischen Groß- und Kleinschreibung unterschieden! Dieses Kennwort sollte nicht vergessen werden!!

Ähnlich wie bei der Server-ID zuvor beschrieben, kann eine bereits existierende Certifier-ID an dieser Stelle verwendet werden. In diesem Fall muss dann das entsprechende Kästchen ausgewählt werden.



Organisationsangaben

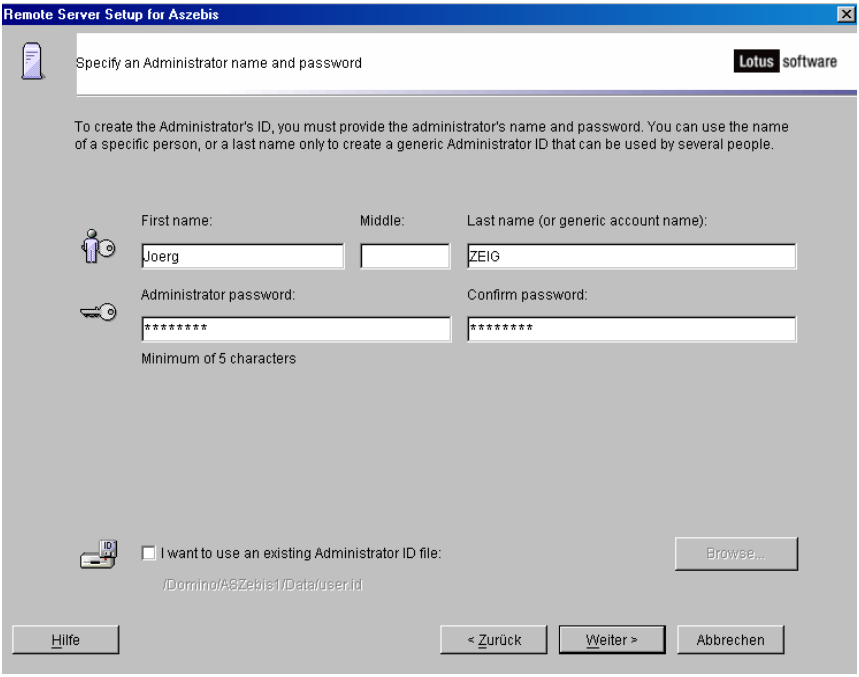
Nun muss die Domino-Domäne eingegeben werden. Dies ist eine Organisationseinheit innerhalb von Domino, deren Bedeutung in Kapitel 1.1 beschrieben ist. In der Praxis bewährt sich hier oft derselbe Name, wie er für die Organisation angegeben wurde.



Domain-Angaben

Der Installationsprozess generiert nun den Domino-Administrator, dessen Name hier angegeben werden kann. Für das Administrationskennwort gilt auch hier: Es wird zwischen Groß- und Kleinschreibung unterschieden!

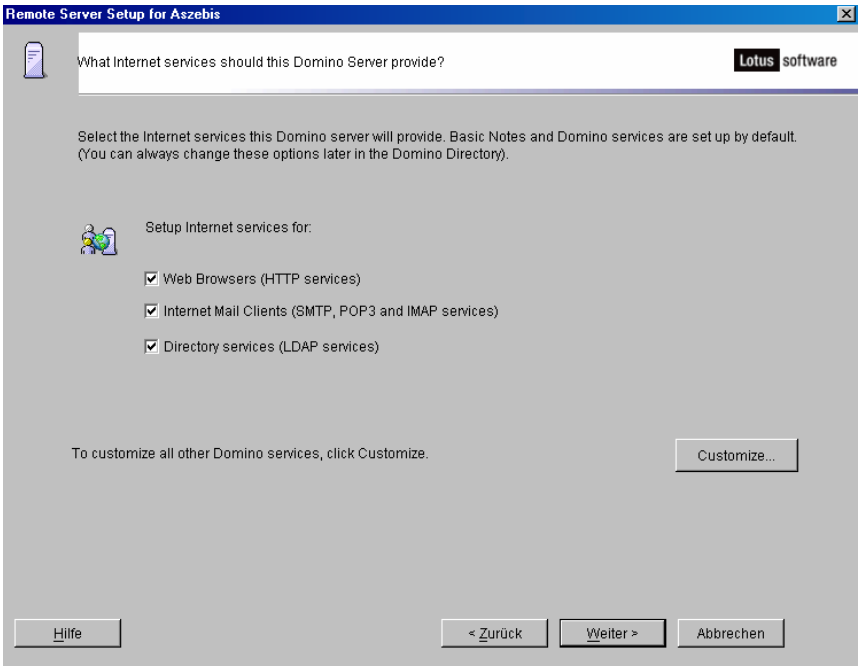
Liegt für den zu installierenden Server bereits eine Administrations-ID vor, kann alternativ zur Namensvergabe das Kästchen für die Verwendung der existierenden ID markiert werden.



Administrator-Angaben

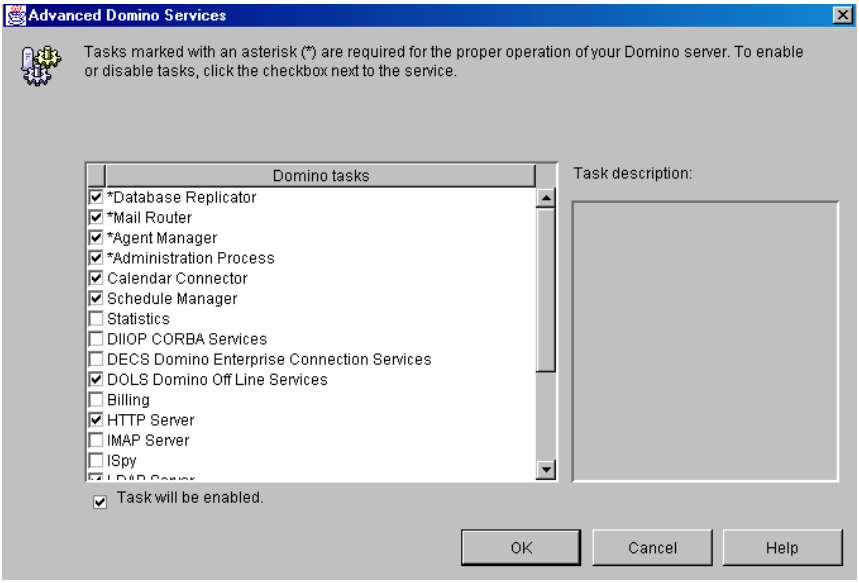
Mit Domino können verschiedene Internet-Dienste genutzt werden. Einige Neuentwicklungen in den Release-Versionen 5 und 6 wurden gerade in diesem Bereich vorgenommen.

Wird der Einsatz von iNotes oder DOLS geplant, dann sollten hier bereits die entsprechenden Angaben gemacht werden. Diese Angaben können aber auch später, nach dem Einrichten des Domino Servers, angepasst werden. iNotes erfordert zum Beispiel den „HTTP Web-Browser“.



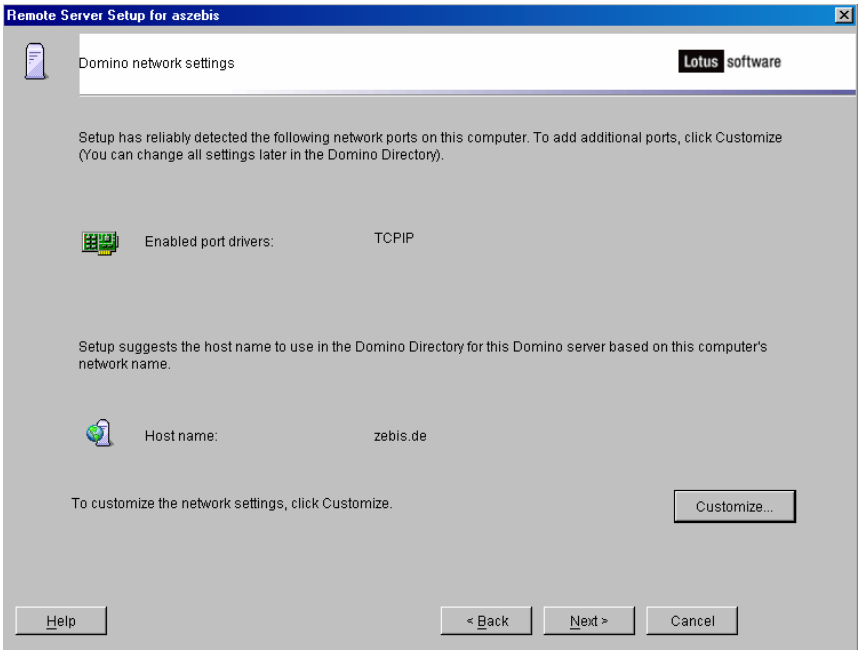
Internet-Services

Um die Standardeinstellungen zu modifizieren, wird die Schaltfläche „Customize…“ ausgewählt. Einträge, die mit einem Stern gekennzeichnet sind, sind für die Grundfunktionen von Domino notwendig und sollten nicht entfernt werden!

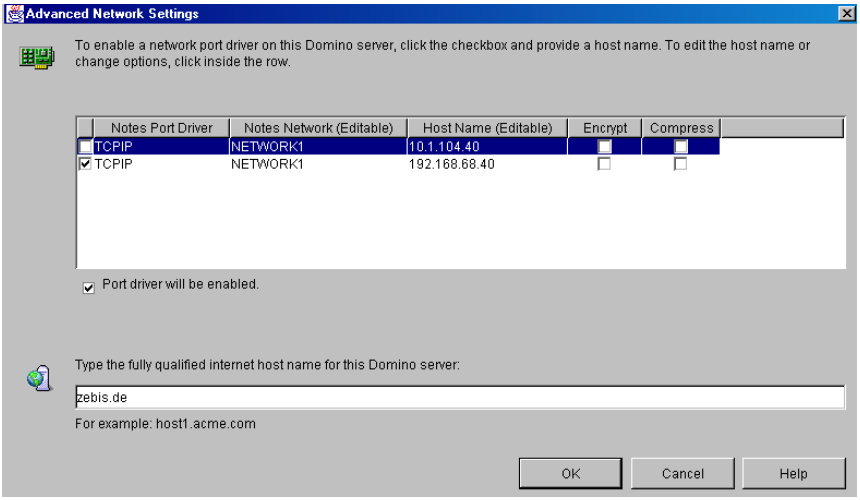


Advanced-Angaben erweitert

Für die Kommunikation müssen nun die Netzwerkeinstellungen definiert werden. Die Kommunikation läuft dabei über TCP/IP. Der Host-Name wird automatisch aus den Definitionen der iSeries ermittelt. Sind auf der iSeries mehrere Schnittstellen vorhanden, kann die gewünschte Schnittstelle nach Auswahl der Schaltfläche „Customize…“ ausgewählt werden.



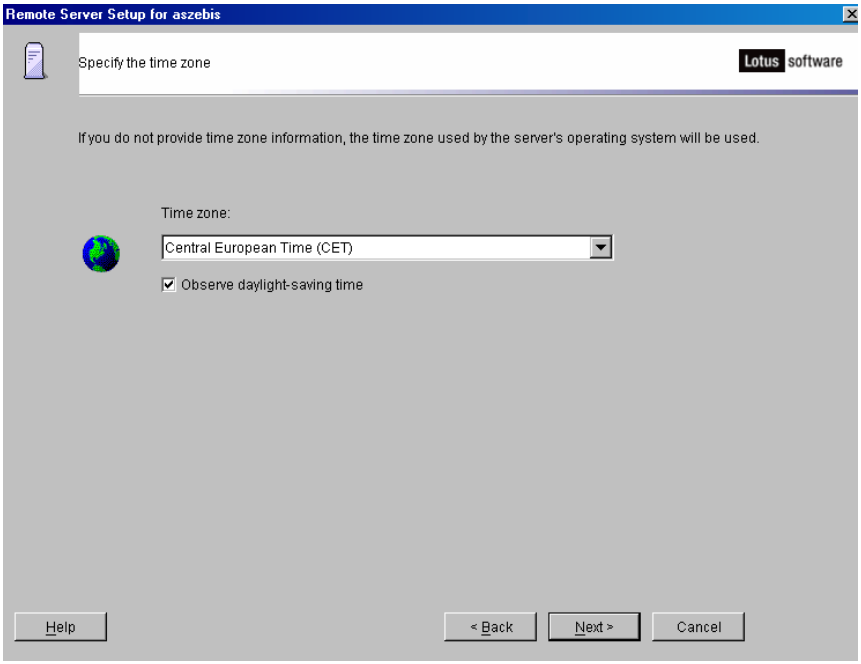
Netzwerkeinstellungen



Erweiterte Netzwerkeinstellungen

In diesem Fall sind auf der iSeries zwei Schnittstellen vorhanden. Es kann nur eine Schnittstelle ausgewählt werden.

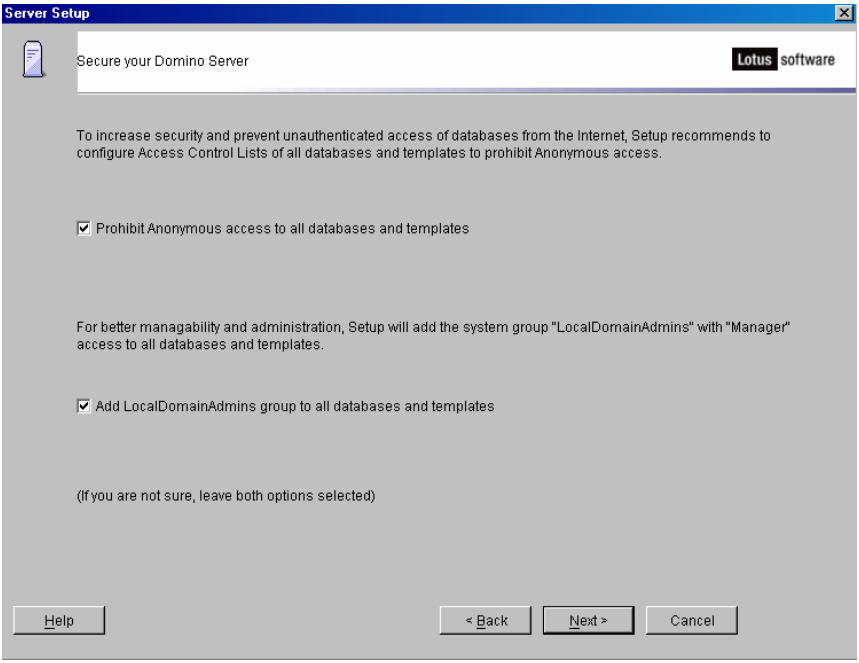
Wichtig bei der Konfiguration ist die Angabe der Zeitzone, in der der Domino-Server betrieben wird. Hintergründe und Bedeutungen dieses Parameters finden sie im Abschnitt „Administration“ in diesem Buch.



Zeitzonenangabe

Ausgehend davon, dass der Domino-Server vor unberechtigten Zugriffen geschützt werden soll, sind per Vorgabe die Sicherheitseinstellungen so gewählt, dass unautorisierte Zugriffe auf Datenbanken innerhalb des Domino-Servers nicht zugelassen werden.

Es empfiehlt sich, die Voreinstellungen zu übernehmen!

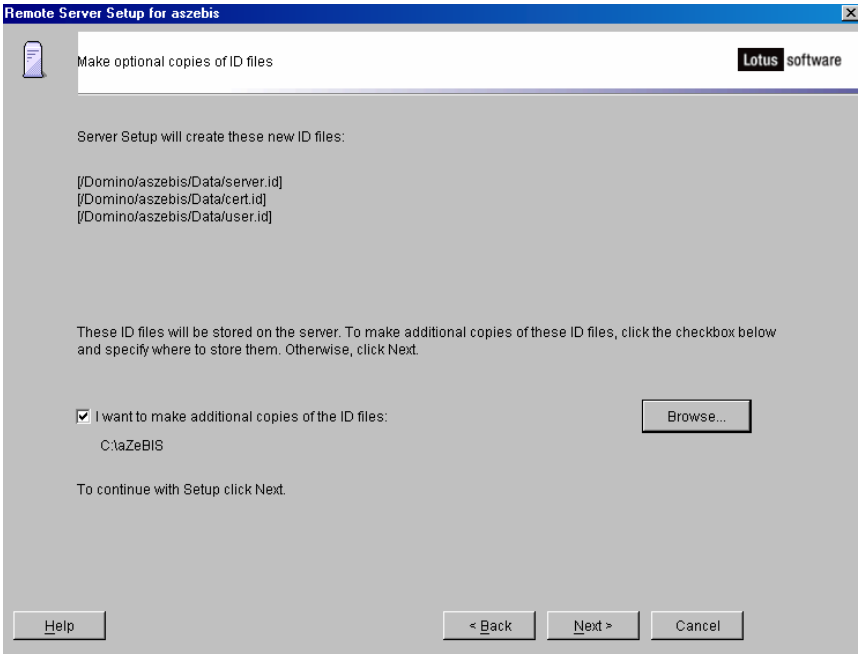


Sicherheitseinstellungen

Im Laufe der Konfiguration werden nun

- die Server ID,
- die Cert ID und
- die Admin ID (User ID)

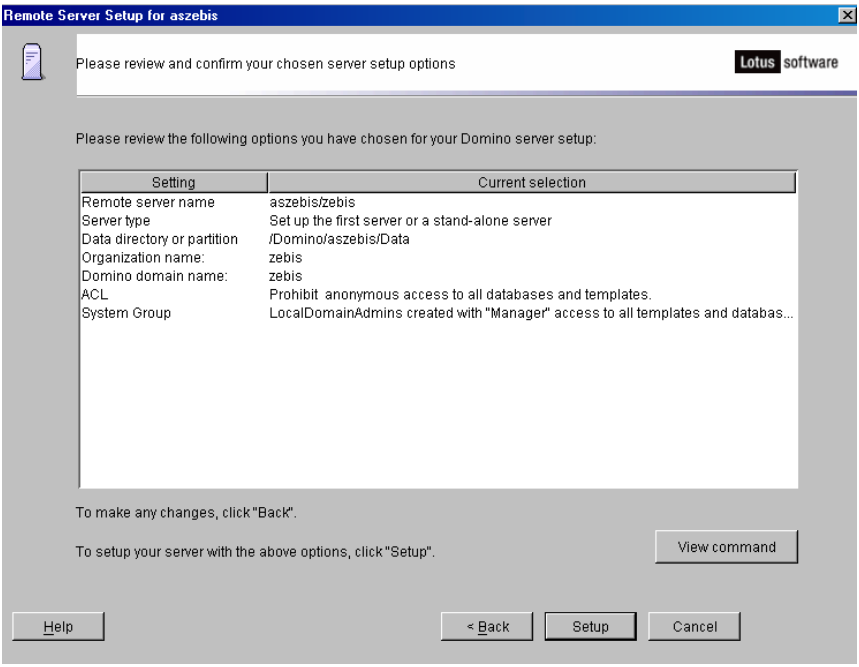
erstellt und in dem vorher angegebenen Domino-Daten-Verzeichnis innerhalb des IFS gespeichert.



Installationsangabe ID File

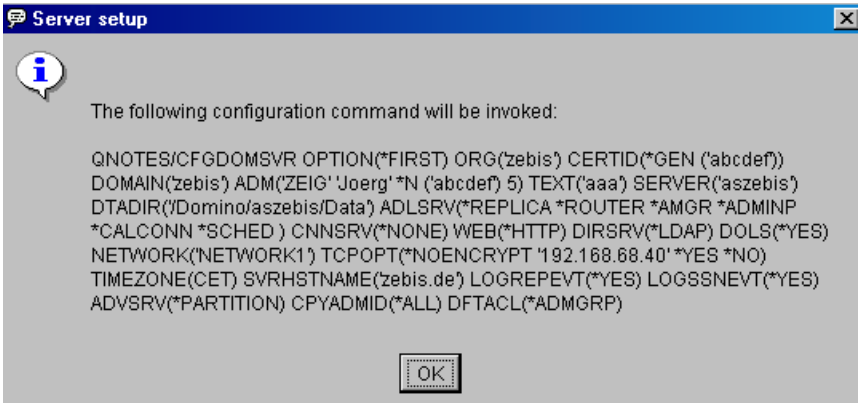
Es empfiehlt sich die optionale Speicherung einer weiteren Kopie. Dazu ist das entsprechende Auswahlfeld zu markieren. Über die Schaltfläche „Browse“ kann ein Verzeichnis innerhalb des Netzwerkes als Speicherort der Kopie der wichtigen ID-Files ausgewählt werden.

Nach Abschluss dieser Eingaben wird eine Zusammenfassung aller bisher getätigten Auswahlen zur abschließenden Prüfung angezeigt. Änderungen können durch Anklicken der Schaltfläche „Back“ und Rücksprung auf die jeweiligen Auswahlfelder durchgeführt werden.



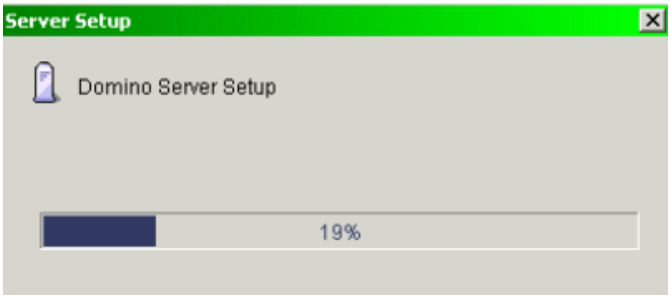
Abschlussbestätigung

Die Schaltfläche „View command“ zeigt den aufbereiteten Befehls-String an, der mit seinen Parametern auch zum Beispiel als Befehl „CFGDOMSVR“ auf OS/400-Ebene eingegeben werden könnte.



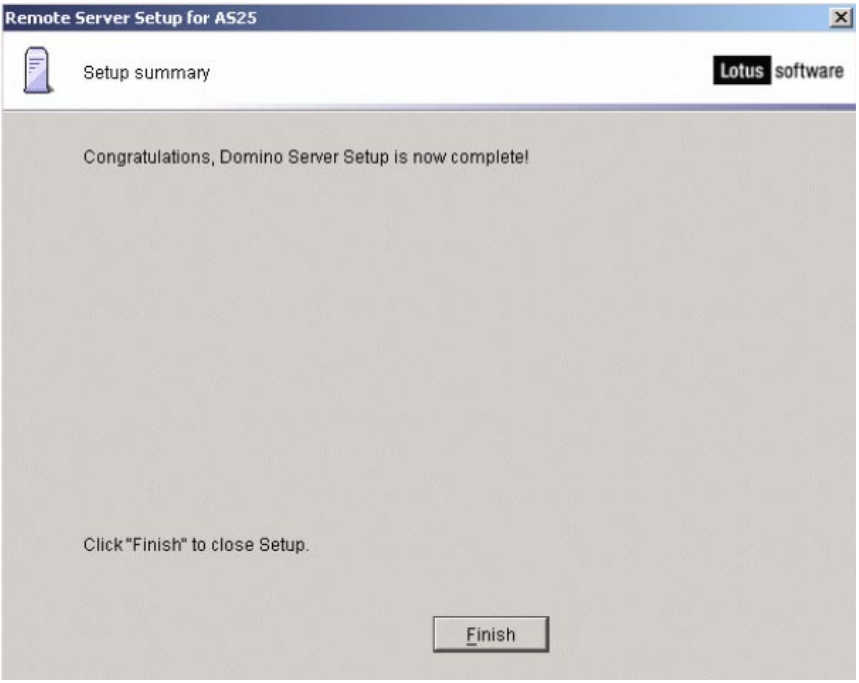
Befehls-String

Soll die Konfiguration des Domino-Servers mit den Einstellungen durchgeführt werden, dann wird diese mit Betätigen der Schaltfläche „Setup“ gestartet und der Status der Installation durch eine Fortschrittsanzeige angezeigt.



Installationsstatus

War die Konfiguration erfolgreich, erscheint die Abschlussmeldung.



Abschlussmeldung

4.2.3 Installation mit iSeries Navigator

Wie bereits im vorhergehenden Kapitel beschrieben, steht neben der 5250-Oberfläche auch der iSeries Navigator (der frühere Operations Navigator) für die Installation zur Verfügung.

Der iSeries Navigator wurde in den letzten OS/400 Release-Versionen ständig erweitert. In einigen Bereichen gibt es sogar Funktionen, die nur noch über den iSeries Navigator ausgeführt werden können. Somit stellt dieses Tool ein immer wichtigeres Werkzeug in der täglichen Administration der iSeries dar, weshalb im Folgenden die Administration von Domino mit dem iSeries Navigator eingehend beschrieben wird.

iSeries Navigator ist ein Bestandteil von iSeries Access (Lizenzprogramm Nummer 5722-XE1). Dieses Lizenzprogramm muss auf der iSeries installiert sein, um die Installation von Domino mit iSeries Navigator durchführen zu können.

Auf dem PC, von dem die Installation durchgeführt werden soll, muss „IBM iSeries Access für Windows“ installiert sein, von dem eine der Komponenten der „iSeries Navigator“ ist.

Die Installation mit dem iSeries Navigator erfolgt dann durch das „InstallShield“, ein Java-basierendes Interface, das plattformübergreifend seit Version 6 die gleiche Installationsoberfläche für die Installation von Domino bietet.

Mit Hilfe dieses Installationsverfahrens kann die Installation:

- grafisch oder
- von dem iSeries CD/DVD-Laufwerk bzw. einem PC-Laufwerk erfolgen.

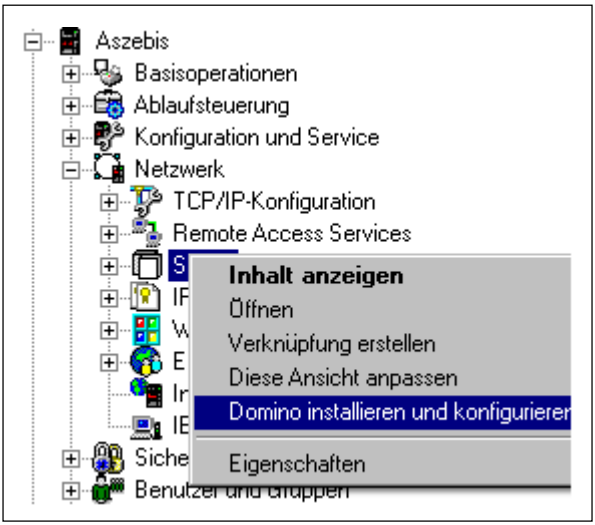
Der Aufruf des InstallShield kann auch durch Ausführen der entsprechenden „Setup.Exe“, die sich auf der CD „Domino für iSeries“ befindet, oder durch Verwendung des iSeries Navigators erfolgen.

Wenn Sie bereits den iSeries Navigator (oder die frühere Bezeichnung Operations Navigator) im Einsatz haben, bietet dieser mit der Option

„Domino Installieren und Konfigurieren“

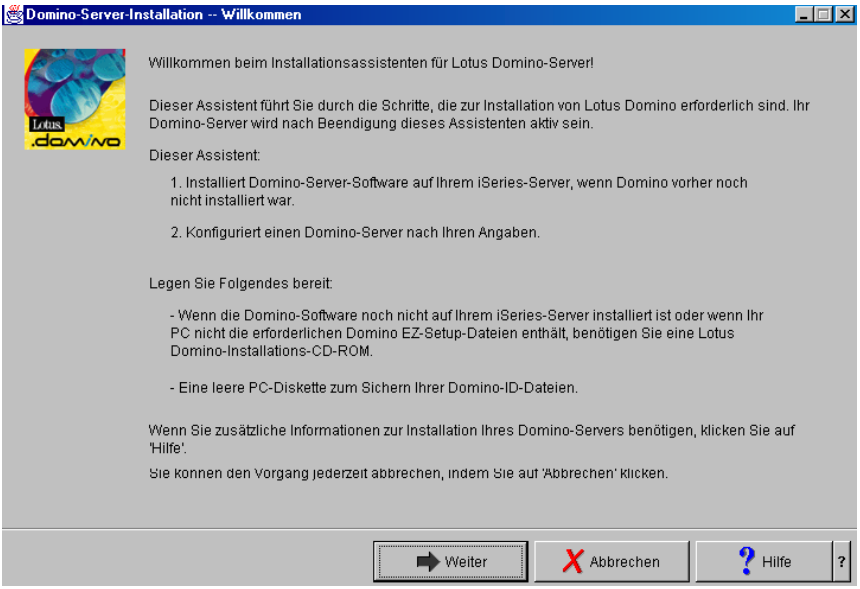
eine elegante Möglichkeit, Domino auf der iSeries zu installieren und zu verwalten. Dieses Installationsverfahren wird nun nachfolgend eingehender beschrieben.

Nach dem Start von iSeries Navigator und der Auswahl des iSeries-Systems, auf dem die Installation erfolgen soll, ist der Eintrag „Netzwerk“ auszuwählen. In dessen Erweiterung befindet sich der Eintrag „Server“. Nach Markieren des Eintrages „Server“ mit der rechten Maustaste erscheint ein Fenster mit einer Option „Domino installieren und konfigurieren“.



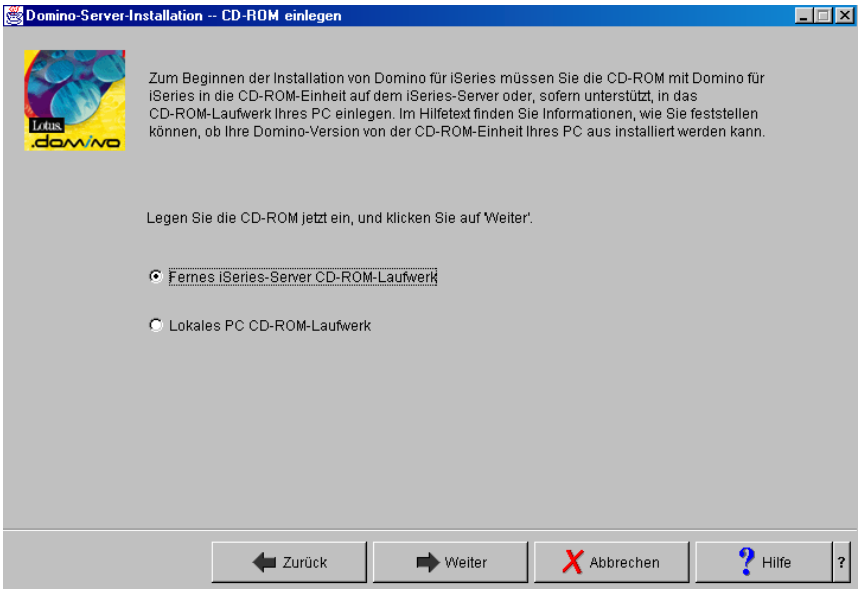
iSeries Navigator „Domino installieren und konfigurieren“

Nach der Auswahl dieser Option wird das InstallShield automatisch gestartet.



Domino-Server-Installation – Willkommen

Nun kann zwischen dem CD/DVD-Laufwerk der iSeries oder einem PC-Laufwerk gewählt werden, von dem aus die Installation erfolgen soll.

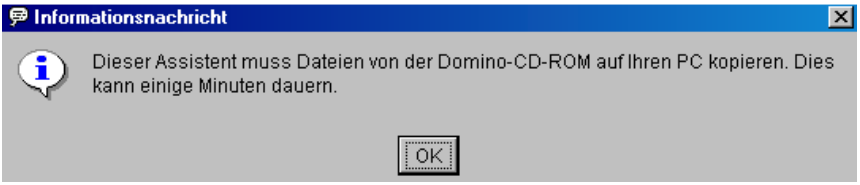


CD-Laufwerk – Auswahl

Befindet sich auf dem System eine andere primäre Sprache, als die der zu installierenden Domino-Software (was bei einer deutschen Installation meistens der Fall ist), dann wird eine Hinweismeldung ausgegeben, die mit „OK“ übergangen werden kann.

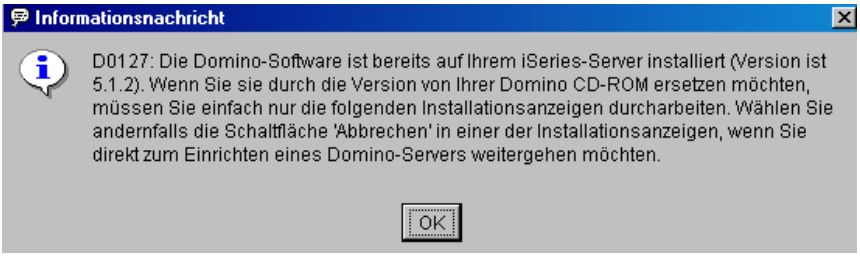
Sprach-Abweichung

Die Installation des Software-Codes auf der iSeries beginnt nun. Lassen Sie sich nicht durch die nachfolgende Anzeige verwirren, die Ihnen mitteilt, dass Daten auf Ihren PC kopiert werden. Tatsächlich werden die Daten auf der iSeries und ihrem File-System installiert.



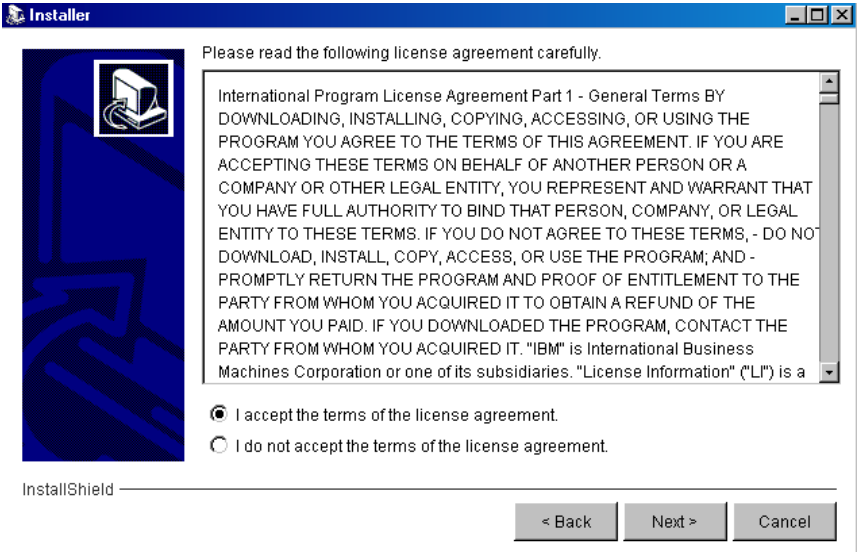
Installationsbeginn

Ist bereits eine frühere Version von Domino auf der iSeries installiert, dann erscheint folgende Hinweismeldung. Beachten Sie bitte, dass bis zur Version 6.0.3 bzw. 6.5 hier in jedem Fall ein Upgrade erfolgt, da alle niedrigeren Versionen kein Multi-Versioning unterstützen!



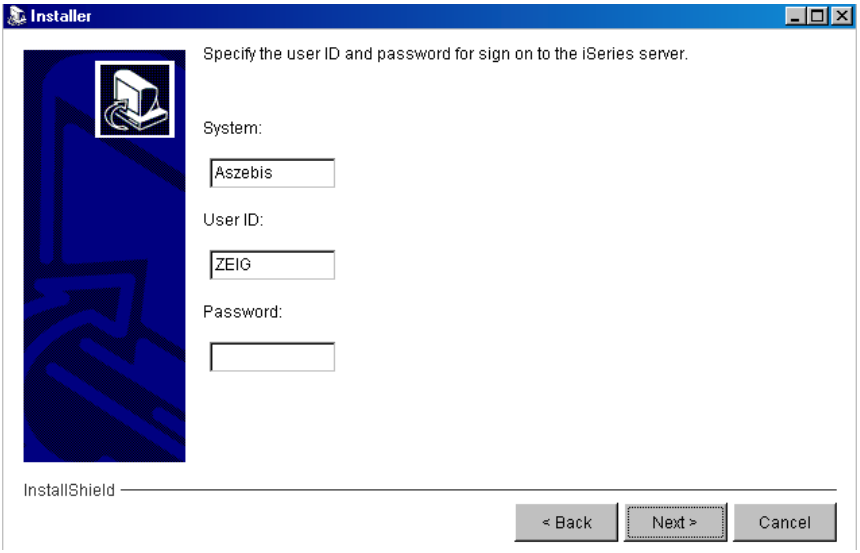
Upgrade-Hinweis

InstallShield Wizard



Lizenzbestimmungen

Um die Installation fortzusetzen sind – wie üblich – die Lizenzbestimmungen zu akzeptieren.



Installer – Anmeldung

In der weiteren Anzeige erfolgt dann die Anmeldung auf der iSeries. Es ist darauf zu achten, dass der Benutzer über ausreichende Berechtigungen für die Installation verfügt.

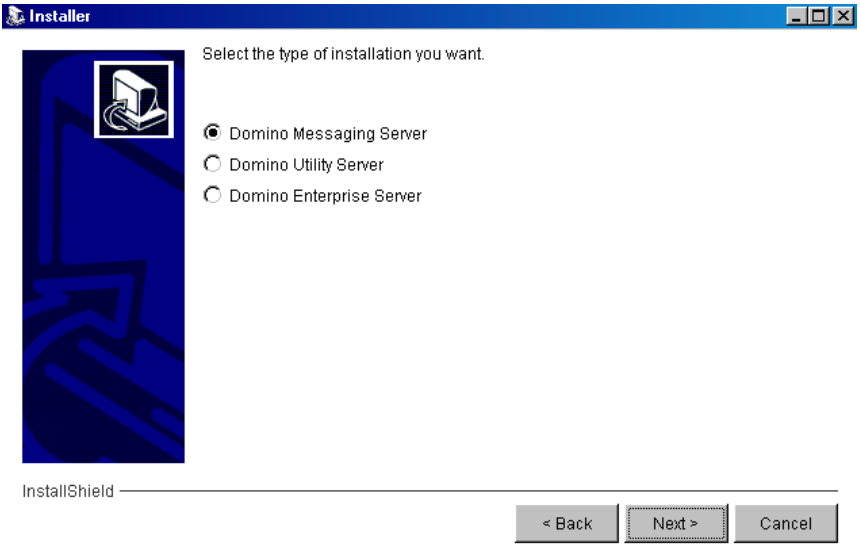
So muss der Benutzer, mit dem hier gearbeitet werden soll, über die Berechtigungen *ALLOBJ, *JOBCTL, *IOSYSCFG und *SECDAM verfügen.

Je nach Lizenztyp ist der jeweilige Servertyp auszuwählen, der installiert werden soll.

- **Domino Messaging Server**
  (frühere Bezeichnung: Mailserver)
  Unterstützt Messaging/Kalenderfunktionen, Persönliches Verzeichnis, Persönliches Journal, Diskussions- und Dokumentenbibliotheken.

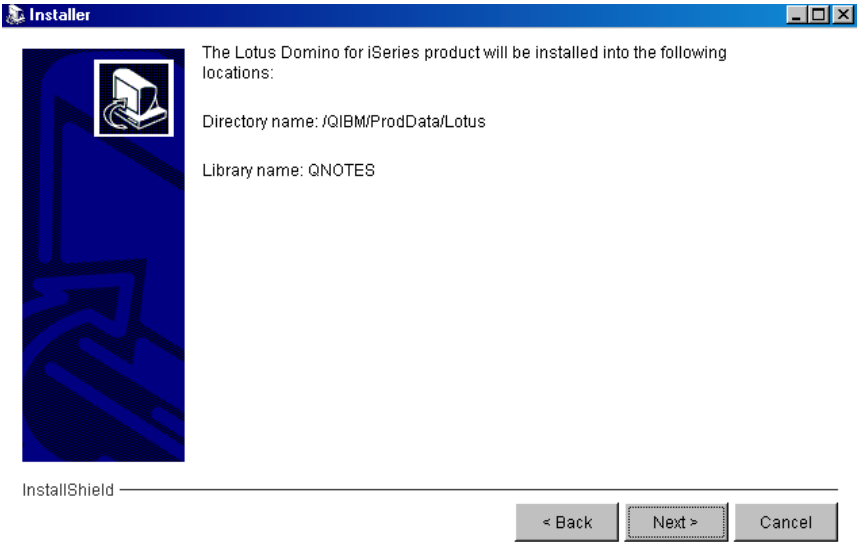
- **Domino Utility Server**
  (frühere Bezeichnung: Extranet Server)
  Ermöglicht das Ausführen von Domino Applikationen, unterstützt jedoch keinen Zugriff auf Notes-Mail-Datenbanken.

- **Domino Enterprise Server**
  (frühere Bezeichnung: Application Server, Enterprise Server, Advanced Enterprise Server)
  Unterstützt dieselben Applikationen wie der Messaging Server und darüber hinaus Team Rooms und kundenindividuelle Applikationen. Ist zudem Voraussetzung für Cluster (z.B. Hochverfügbarkeitslösungen).


Installer
Select the type of installation you want.
Domino Messaging Server
Domino Utility Server
Domino Enterprise Server
InstallShield
< Back
Next >
Cancel

Server-Typ

Die nächste Anzeige ist rein informativ und zeigt die Pfadangabe für die Domino-Installation und die während der Installation anzulegende Bibliothek QNOTES.

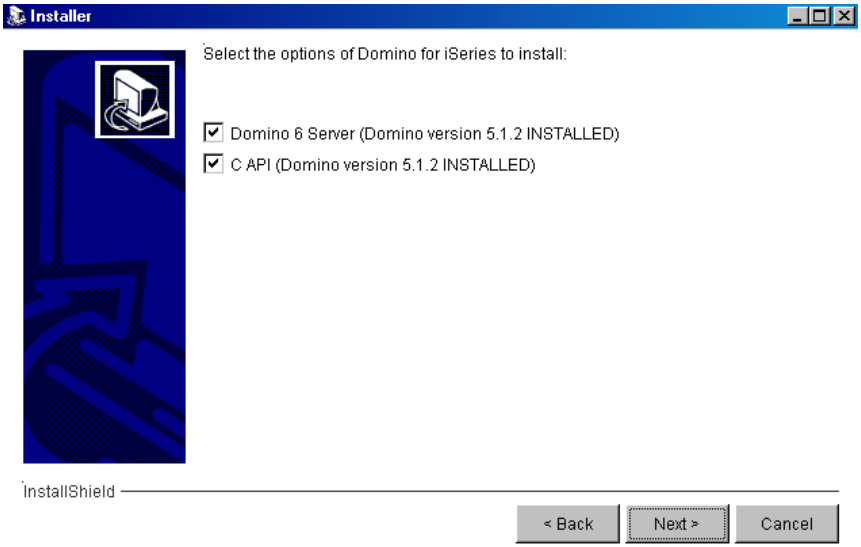


Installationspfad

Es kann nun ausgewählt werden, ob nur die Basisinstallation oder auch die Erweiterung in Form der C-API installiert werden soll. Im Unterschied zu den bisherigen Release-Versionen, bei denen bis zu sieben unterschiedliche Optionen installiert werden konnten, stehen seit dem Release 6 noch zwei Optionen zur Verfügung, wobei die frühere Option „Advanced Services“ mit in die Basis-Option integriert wurde.

- **Domino-Server (Option *BASE)**
  Enthält Programme, Daten und Schablonendateien, die zum Ausführen des Domino-Servers notwendig sind, sowie den SMTP Support, DECS, den HTTP-Server sowie die Hilfe-Datenbanken. Diese Option ist Grundvoraussetzung für die C-API-Option und muss installiert werden.

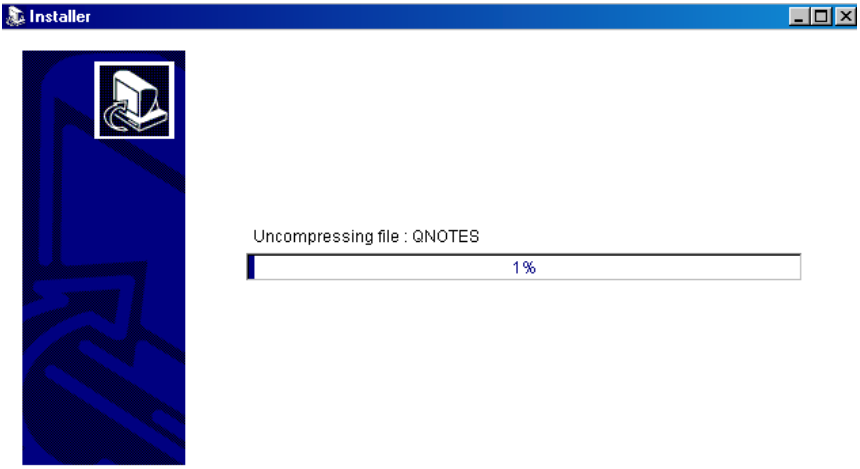
- **C API (Option 1)**
  Ist notwendig für das Erstellen von C-Anwendungen in Notes, die auf der iSeries ausgeführt werden.



Installationsoptionen

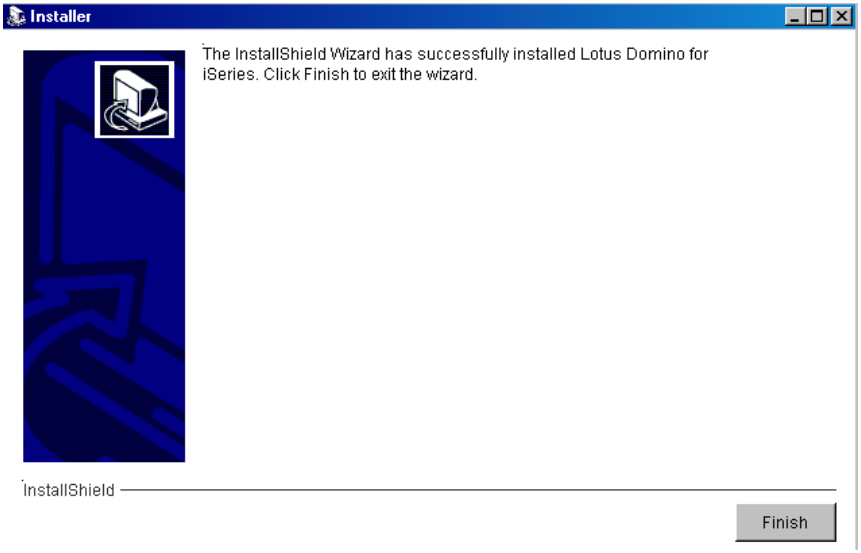
Nach der Auswahl kommt nochmals ein Bestätigungsfenster, bevor der Installationscode von der CD auf das System kopiert wird.

Je nach Performance der Maschine kann der Fortschritt der Installationsanzeige hin und wieder „hängen“, was damit zusammenhängt, dass im Zuge der Installation die Daten auf der iSeries entpackt werden müssen.



Installationsstatus

Wurde die Installation erfolgreich abgeschlossen, erscheint eine Meldung, die dann mit „Finish“ abgeschlossen werden kann.



Abschluss der Installation

Damit ist die Installation des Domino-Codes erfolgt.

Als Nächstes muss nun die Konfiguration durchgeführt werden, die automatisch nach der Installation mit dem InstallShield Wizard startet. Die Konfiguration kann auch später vorgenommen werden. Es erfolgt in jedem Fall eine Prüfung, ob der Installationscode zuvor installiert wurde.

Zum späteren Aufruf kann die Konfiguration über den bekannten Weg im iSeries Navigator, über EZ Setup oder über den Befehl CFGDOMSVR erfolgen.

Details dazu finden Sie im weiteren Verlauf dieses Kapitels.

4.2.4 Multi-Versioning

Lotus Domino auf der iSeries unterscheidet sich in einigen Bereichen von der Installation auf anderen Server-Plattformen. Neben einigen Vorteilen bei dem Einsatz dieser Server-Version sind allerdings auch einige Einschränkungen zu nennen. Einer der wesentlichen Einschränkungen wurde mit Erscheinen der Release-Versionen 6.0.3 und 6.5.0 mit dem so genannten Multi-Versioning beseitigt. Darunter versteht man die Möglichkeit, zeitgleich mehrere unterschiedliche Domino-Release-Versionen parallel auf einer iSeries installieren und betreiben zu können.

Bedingt durch die Architektur der iSeries und der Integration von Domino war bisher die Installation unterschiedlicher Domino-Release-Versionen auf einer iSeries nicht möglich. Dies hängt damit zusammen, dass die notwendigen Objekte nur in bestimmten Bibliotheken oder Verzeichnissen gespeichert werden, die nur einmalig auf dem System existieren dürfen und die keine Release-abhängigen Informationen enthalten. Diese Beschränkung wurde mit Einführung von Multi-Versioning beseitigt und der Installationsprozess dahingehend angepasst, dass Domino Release-abhängige Objekte nun in unterschiedlichen Versionen – getrennt in den jeweiligen Bibliotheken und Verzeichnissen – parallel auf einer iSeries innerhalb einer LPAR installiert werden können.

Bisher war es nicht möglich, die im Vorfeld eines Domino Release-Wechsels erforderlichen Umstellungstests durchzuführen. Obwohl oder gerade weil Domino für unterschiedliche Server-Plattformen zur Verfügung steht, unterscheiden diese sich in einigen Punkten doch stark: Zum Beispiel kann der Ablauftest ei-

ner Domino-Anwendung, die eigentlich auf einer iSeries laufen sollte, nicht zweifelsfrei auf einer anderen beliebigen Domino Server-Variante (z.B. Windows) getestet werden.

Nachfolgend wird auf die Details des Multi-Versioning näher eingegangen.

Anmerkung:
Multi-Versioning ersetzt nicht in jedem Fall die Installation von Domino in unterschiedlichen LPAR-Umgebungen.

Bei nachfolgenden Konstellationen ist die Installation in einzelnen LPARs notwendig:

- bei der Unterstützung unterschiedlicher OS/400 Release-Versionen,
- bei unterschiedlichen TCP/IP-Konfigurationen,
- bei besonderen Systemwert-Einstellungen,
- bei notwendigen, spezifischen Anpassungen an dem Benutzerprofil QNOTES.

Neben den bekannten und in Kapitel 4.2.2 im Detail beschriebenen Anforderungen für die Installation von Domino auf der iSeries sind bei der Installation von Multi-Versioning-fähigen Releases zusätzlich einige Voraussetzungen zu erfüllen.

Soll Multi-Versioning genutzt werden, dann ist zu beachten, dass alle parallel auf der iSeries zu installierenden Domino Release-Versionen Multi-Versioning-fähig sind. Ist auf einer iSeries ein Domino-Server mit einem Release-Stand installiert, der nicht Multi-Versioning-fähig ist, dann muss dieser Server zunächst auf einen Multi-Versioning-fähigen Release-Stand angehoben werden, um anschließend weitere Domino-Server mit anderen, ebenfalls Multi-Versioning-fähigen Release-Versionen installieren zu können!

Ist zum Beispiel der Release-Stand des Domino-Servers 5.0.12 und soll parallel ein Server mit dem Release-Stand 6.0.3 installiert werden, dann wird die Parallel-Installation des Domino 6.0.3 scheitern, da während des Installationsprozesses geprüft wird, ob alle bereits installierten Domino-Server den korrekten Multi-Versioning-fähigen Stand haben. In einem solchen Fall würde nur ein Upgrade des bereits installierten Servers möglich sein – und dies auch nur dann, wenn es einen von IBM und Lotus unterstützten Upgrade-Pfad gibt.

Die nachfolgende Übersicht veranschaulicht die Multi-Versioning-Fähigkeit der aktuellen Domino Release-Versionen, die auf einer iSeries installiert werden können. Alle in der letzten rechten Spalte mit einem „X“ markierten Release-Versionen sind Multi-Versioning-fähig.

Domino Release	Gleiche OS/400 Partition	Gleiche OS/400 Partition	Gleiche OS/400 Partition	Gleiche OS/400 Partition	Gleiche OS/400 Partition
5.0.x 5769-LNT	X	-	-	-	-
6.0.0 5733-LD6	-	X	-	-	-
6.0.1 5733-LD6	-	-	X	-	-
6.0.2 5733-LD6	-	-	-	X	-
6.0.3 5733-LD6	-	-	-	-	X
6.0.3.x 5733-LD6	-	-	-	-	X
6.5.0 5733-L65	-	-	-	-	X
6.5.0.x 5733-L65	-	-	-	-	X

Release-Übersicht

Im Zuge der Einführung des Multi-Versioning mussten einige Anpassungen im Bereich der OS/400-Integration vorgenommen werden, damit die Verarbeitung mehrerer unterschiedlicher Domino Release-Versionen möglich wird. Nachfolgend wird zunächst auf die OS/400-Anpassungen eingegangen.

Bisher wurden die Objekte, die die Integration von Domino auf der iSeries ermöglichen, in unterschiedlichen, Domino Release-unabhängigen Bibliotheken und Verzeichnissen gespeichert. Durch das im Zuge von Multi-Versioning erforderliche mehrfache Vorhandensein

gleicher oder ähnlicher Objekte, die für die unterschiedlichen Release-Stände notwendig sind, müssen diese Objekte nun Release-abhängig gespeichert werden. Dazu wird auf der iSeries für jedes Domino-Release eine eigene Bibliothek und ein entsprechendes Verzeichnis genutzt, in das die Release-abhängigen Objekte gespeichert werden. Die Release-spezifische Bibliothek wird im späteren Verlauf bei der Konfiguration wie auch beim Betreiben des Servers diesem zugeordnet.

Eine solche Zuordnung kann wie in der nachfolgend gezeigten Bibliotheksliste aussehen. Diese Bibliotheksliste stammt von dem Domino Server-Job. Dieser Server ist Multi-Versioning-fähig und ist mit der Domino Release-Version 6.5.0 installiert.

- **Man beachte**:
  Die Release-spezifische Bibliothek QDOMINO650 steht vor der Release-unabhängigen Bibliothek QNOTES!

```
                    Bibliotheksliste anzeigen
                                                          System:   ASZEBIS
Job:   SERVER          Benutzer:   QNOTES          Nummer:   013194

Auswahl eingeben und Eingabetaste drücken.
  5=Objekte in Bibliothek anzeigen

Aus-
wahl  Bibliothek  Art       ASP-Einheit  Text
      QSYS        SYS                    Systembibliothek
      QSYS2       SYS                    Systembibliothek für CPIs
      QHLPSYS     SYS
      QUSRSYS     SYS                    System Library for Users
      QSYS2924    SYS
      QDOMINO650  USR
      QNOTES      USR
      QGPL        USR                    General Purpose Library
      QTEMP       USR



Ende
 F3=Verlassen   F12=Abbrechen   F16=Jobmenü   F17=Anfang   F18=Ende
 (C) COPYRIGHT IBM CORP. 1980, 2002.
```

Bibliotheksliste

Bei der Installation von mehreren Release-Versionen werden die Domino-Objekte in unterschiedlichen Bibliotheken und Verzeichnissen gespeichert:

- Release-unabhängige Informationen für die Domino-Integration
  - Bibliothek QSYS
  - Bibliothek QNOTES
  - Verzeichnis /QIBM/ProdData/LOTUS/NOTES
- Release-abhängige Informationen für die Domino Integration
  - Bibliotheken
    - QDOMINO60x (für Domino Versionen 6.0.x)
    - QDOMINO65x (für Domino Versionen 6.5.x)
  - Verzeichnisse
    - /QIBM/ProdData/LOTUS/DOMINO60x
    - /QIBM/ProdData/LOTUS/DOMINO65x

Wie im weiteren Verlauf näher erläutert wird, ist es wichtig, dass in einer Multi-Versioning Umgebung die jeweilige Release-abhängige Bibliothek (z.B. QDOMINO650) vor der Bibliothek QNOTES steht, die globale Release-unabhängige Objekte enthält!

Werden Release-abhängige Befehle verwendet, dann wird ohne eine spezifische Angabe der Bibliothek, aus der dieser Befehl aufgerufen werden soll, der jeweilige Befehl aus der Bibliothek QSYS bzw. QNOTES verwendet. Soll eine Befehlsvariante aus einer anderen Bibliothek – also mit einem anderen Release-Stand – verwendet werden, dann muss die Befehlseingabe explizit mit kompletter Pfadangabe erfolgen. Generell gilt, dass bei der Angabe eines

Befehls ohne explizite Pfadangabe die Befehlsversion des Primary-Servers verwendet wird. Unter dem Primary-Server versteht man den Domino-Server, der den höchsten Installationslevel hat und der die Release-unabhängigen Domino-Informationen (z.B. Befehle) in den Bibliotheken QSYS und QNOTES liefert. Details zu dem Primary-Server bzw. zu dem Primary-Release finden Sie im weiteren Verlauf dieses Kapitels.

Beispiel:

- CHGDOMSVR DOMSVR1
  - Dieser Befehl wird aus der Bibliothek QSYS gestartet.
- QDOMINO603/DOMSVR1
  - Dieser Befehl wird aus der explizit angegebenen Bibliothek QDOMINO603 verwendet.

Die Primary-Version dieser Befehle befindet sich zwar – wie zuvor beschrieben – nach wie vor in der Bibliothek QSYS, wird aber im Zuge jeder Installation einer Multi-Versioning-Version auch in die entsprechenden Domino Release-Bibliotheken (z.B. QDOMINO650) kopiert.

Bei der Konfiguration eines Domino Servers in einer Multi-Versioning-Umgebung muss der Aufruf des Befehls „CFGDOMSVR“ qualifiziert mit der Bibliotheksangabe erfolgen, da im Zuge der Konfiguration keine Domino Release-Angabe möglich ist.

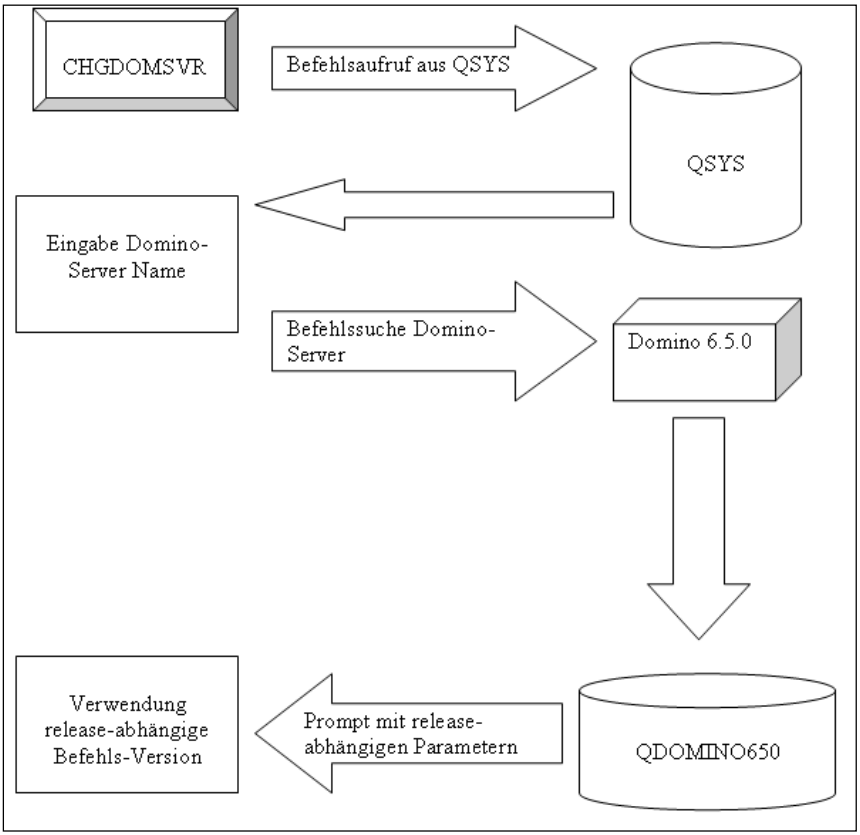
Als Beispiel: „QDOMINO650/CFGDOMSVR“

Anmerkung:
Bei der Konfiguration eines Servers mit einem Primary-Release kann die Angabe des Befehls CFGDOMSVR auch ohne Angabe der Installationsbibliothek erfolgen, da der zu verwendende Befehl als Primary-Version in die Bibliothek QSYS gestellt wurde.

Bei einigen Domino-Befehlen wird die zu verwendende Befehls-Version anhand des Domino-Servers automatisch ermittelt.

Wird zum Beispiel der Befehl „CHGDOMSVR“ ohne qualifizierte Bibliotheksangabe verwendet, so wird der Befehl aus der QSYS herangezogen. Durch die anschließend notwendige Eingabe des Domino-Servers wird dessen Stand ermittelt und im weiteren Verlauf wird der zu diesem Domino-Server zugehörige Befehl aus der jeweiligen QDOMINOxxx-Bibliothek verwendet.

Die nachfolgende Übersicht stellt schematisch den Ablauf einer Befehlseingabe sowie der korrekten Versionsermittlung und Versionsverwendung in einem Multi-Versioning-Umfeld dar:



Befehlsfindung

Für die Domino Integration ist es nach wie vor erforderlich, dass einige Objekte Domino Release-unabhängig auf der iSeries angelegt werden. Diese Objekte dienen der allgemeinen Verwal-

tung und Administration von Domino. Die nachfolgende Übersicht zeigt einige der Domino Release-unabhängigen Befehle auf der iSeries:

- WRKDOMSVR (Arbeiten mit Domino-Servern)
- STRDOMSVR (Starten von Domino-Servern)
- ENDDOMSVR (Beenden von Domino-Servern)
- WRKDOMCSL (Arbeiten mit der Domino-Konsole)
- DSPDOMSCSL (Anzeigen der Domino-Konsole)
- ADDDOMAPP (Hinzufügen von Domino-Anwendungen)
- SETDOMENV (Definieren des Domino-Enviroments)

In dem Installationsprozess von Domino ist jeweils festgelegt, welche Domino-Version die Primary- oder Master-Version ist, die die allgemeinen Domino-Objekte liefert. Das Einspielen beziehungsweise Ersetzen dieser Release-unabhängigen Objekte wird automatisch während des Installationsprozesses vorgenommen.

4.2.4.1 Lizenzprogramme und Optionen

Bisher wurde die Installation des Domino-Servers als Lizenzprogramm unter den Domino 5 Servern mit dem Feature Code 5769-LNT klassifiziert. Die Domino 6.0.x Server tragen den Feature Code 5733-LD6.

Die Domino-Server mit dem Release-Stand 6.5.x werden unter dem Feature Code 5733-L65 geführt.

Wie auch die älteren Domino-Versionen unterscheiden sich die Multi-Versioning-Ausführungen durch unterschiedliche Optionen. Die Optionen der früheren Release-Versionen sind im Detail im Kapitel 4.2.2. ff. beschrieben. Deshalb wird an dieser Stelle nur auf die Optionen der Multi-Versioning-Versionen eingegangen.

Für Release 6.0.x lauten die Optionen:

Release	Option
6.0.3	13
6.0.4	14
6.0.5	15

Für Release 6.5.x lauten die Optionen:

Release	Option
6.5.0	10
6.5.1	11
6.5.2	12

Bei den bisherigen Domino 6 Release-Versionen, die nicht Multi-Versioning-fähig sind, gibt es zwei Sicherungsdateien (Savefiles), die den zu installierenden Code des Servers beinhalten:

- QNOTES
  - Basis Installation
- QNOTESAPI
  - Option 1 (C-API)

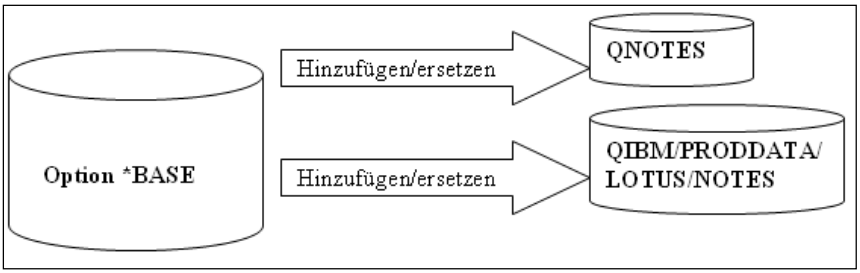
Die Multi-Versioning-fähigen Varianten haben eine zusätzliche Sicherungsdatei, welche die versionsabhängigen Informationen enthält. Diese Sicherungsdatei trägt die Bezeichnung „QNOTESRL“ und stellt den Hauptbestandteil der Installation dar.

Die Abhängigkeit der Installationsquellen zu den späteren Objekten auf der iSeries stellen sich wie folgt dar:

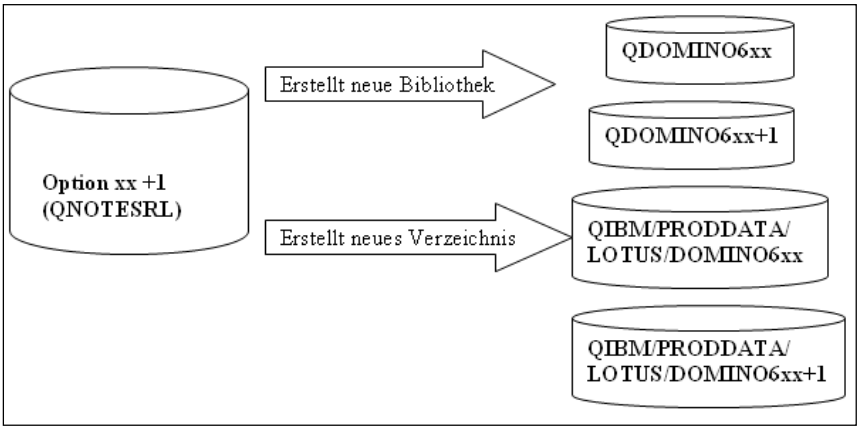
- RSTLICPGM Option *BASE
  - Erstellen der Bibliothek QNOTES
  - Anlegen und Füllen des Verzeichnisses QIBM/PRODDATA/LOTUS/NOTES
- RSTLICPGM Option 1
  - Erstellen der Bibliothek QNOTESAPI
  - Anlegen und Füllen des Verzeichnisses QIBM/PRODDATA/LOTUS/NOTESAPI
- RSTLICPGM Option ‚xxx’ *
  - Erstellen der Bibliothek QDOMINOxxx

– Anlegen und Füllen des Verzeichnisses QIBM/PRODDATA/LOTUS/NOTES/DOMINO6xxx

„xx“ ist der Platzhalter für das jeweilige Release (z.B. QDOMINO650 für Release 6.5.0).



*1 Option *BASE*



Produkt-Option

Wie in der Grafik dargestellt, wird im Zuge der Installation der Release-spezifischen Objekte für jedes Release eine eigene Bibliothek “QDOMINO6xx” sowie eigene Verzeichnisse “QIBM/PRODDATA/LOTUS/DOMINO6xx” angelegt, in die die Release-spezifischen Informationen gespeichert werden.

4.2.4.2 Installation Multi-Versioning Server

Für die Installation von unterschiedlichen Multi-Versioning Servern ist es unerheblich, welche Release-Version zuerst installiert wird. Es ist lediglich darauf zu achten, dass alle auf der iSeries bereits installierten oder zu installierenden Domino Release-Versionen Multi-Versioning-fähig sind.

So können zum Beispiel als erster Server ein Domino 6.5 auf der iSeries installiert werden und anschließend ein zweiter Server mit der Release-Version 6.0.3. Das umgekehrte Verfahren ist ebenfalls möglich.

Ist auf einer iSeries ein nicht Multi-Versioning-fähiges Domino-Release installiert, dann wird durch die Installation zunächst ein Upgrade aller vorhandenen Domino-Server durchgeführt. Eine Parallelinstallation von früheren, nicht Multi-Versioning-fähigen Release-Versionen und Multi-Versioning Release-Versionen ist nicht möglich.

Bei der Installation eines Multi-Versioning-fähigen Domino-Servers auf einer iSeries können – wie bei der Installation früherer Domino-Releases auch – unterschiedliche Installationsverfahren verwendet werden, die zum Teil bereits in den vorhergehenden

Kapiteln eingehend behandelt worden sind.

Als Installationsverfahren können verwendet werden:

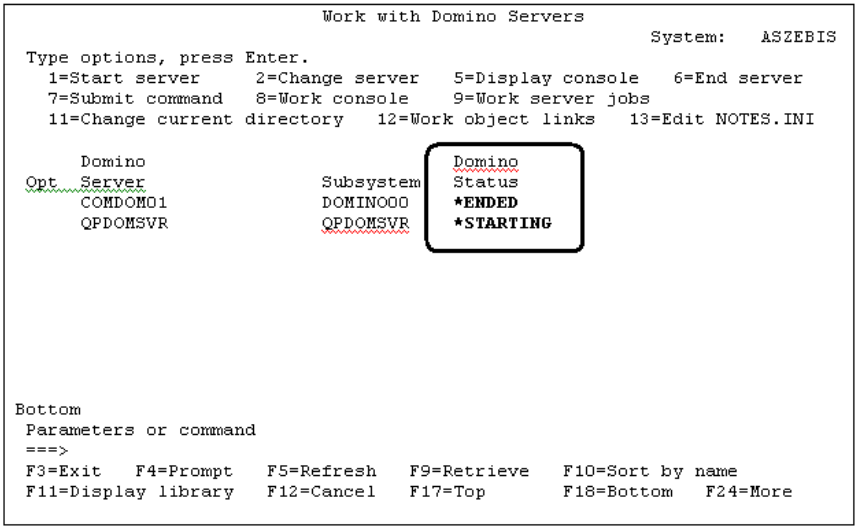
- InstallShield (oder InstallWizard)
  - Durch Aufruf der setup.exe
  - Durch Aufruf aus dem iSeries Navigator
- OS/400-Befehl LODRUN
- OS/400-Befehl RSTLICPGM

In dem nachfolgenden Beispiel werden zwei gängige Verfahren demonstriert, mit denen in einer Partition zwei Domino-Server mit unterschiedlichen Release-Ständen parallel installiert werden.

Dieses Beispiel kann in der Praxis auch angewendet werden, wenn ein bereits installierter Domino-Server zunächst auf ein Multi-Versioning-fähiges Release angehoben werden soll. Dabei müssen die Voraussetzungen für einen Release-Update erfüllt sein.

Unter anderem ist bei einem Release-Update darauf zu achten, dass alle Domino-Server, die auf der iSeries installiert sind, vor dem Update beendet werden.

Ist nicht sicher, welchen Status der Server hat, kann dieser mit dem Befehl „WRKDOMSVR“ ermittelt werden. Alle Server sollten in dieser Anzeige den Status „*ENDED“ haben. Ist dies nicht der Fall, dann muss der Server zunächst beendet werden, bevor der Upgrade erfolgen kann.

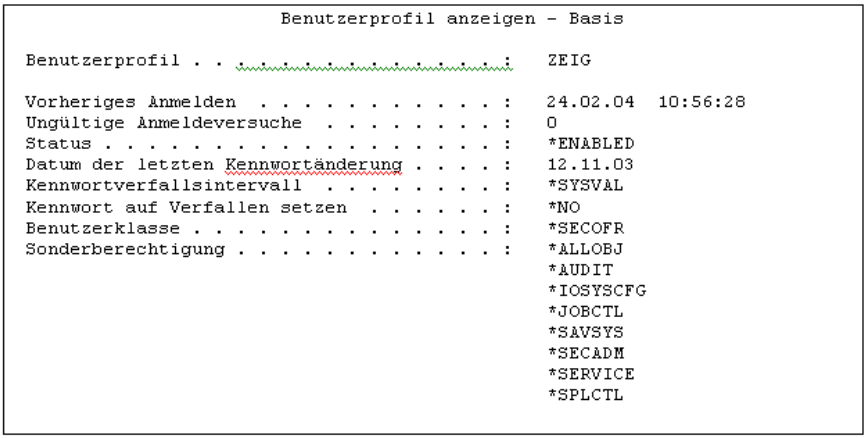


WRKDOMSVR

Für die Installation ist es notwendig, dass der Benutzer, der die Installation und die anschließende Konfiguration durchführt, mindestens über nachfolgende Berechtigungen verfügt:

- *ALLOBJ
- *SECADM
- *IOSYSCFG
- *JOBCTL

Die Berechtigungen können über den Befehl „DSPUSRPRF UserID“ nachgesehen werden.



Berechtigungen anzeigen

Sollen die Berechtigungen erweitert werden, so kann dies mit dem Befehl „WRKUSRPRF UserID“ erfolgen. Vor dem Anpassen der Berechtigungen eines Benutzerprofils sollte auf jeden Fall der Administrator zu Rate gezogen werden.

Ist es nicht sicher, welcher Benutzer ausreichende Berechtigungen zur Installation der Software hat, empfiehlt sich die Verwendung des Benutzers „QSECOFR“ für die Installation.

Für das gezeigte Beispiel sind im Vorfeld als Ausgangvoraussetzungen in Form der erforderlichen Lizenzprogramme PTF, Berechtigungen und sonstige Informationen geprüft worden.

Um die unterschiedlichen Installationsverfahren in diesem Band möglichst komplett darstellen zu können, werden in diesem Beispiel zwei unterschiedliche Verfahren verwendet, die natürlich nicht bindend mit der Installation der jeweiligen Variante sind!

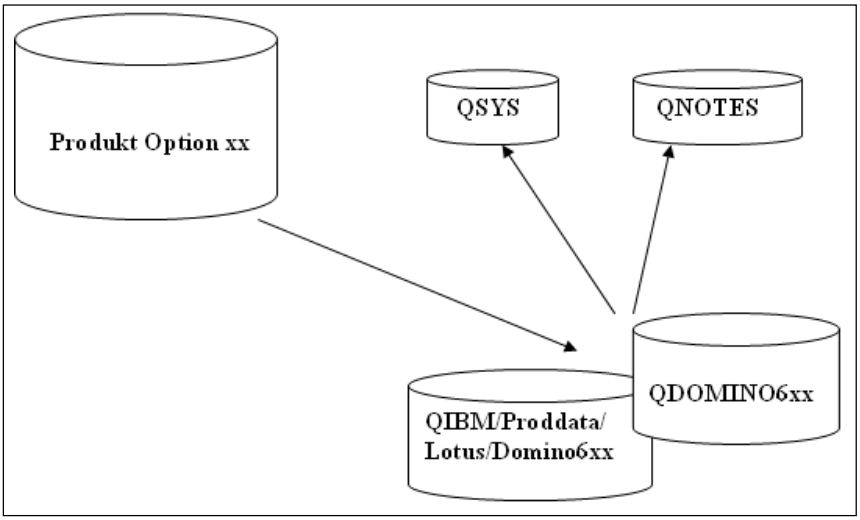
Der Installationscode des ersten Domino-Releases (6.5.0) wurde für dieses Beispiel von der IBM Web-Seite heruntergeladen und steht nun auf einem PC für die Installation zur Verfügung.

Das zweite Domino-Release (6.0.3) liegt auf den originalen Installations-CDs vor und wird über das interne CD/DVD-Laufwerk der iSeries installiert.

Bei diesem Beispiel wird bewusst auf die Installation der sprachspezifischen Versionen verzichtet.

4.2.4.2.1 Installation Multi-Versioning Release 1

Ist auf einer iSeries eine nicht Multi-Versioning-fähige Release-Version installiert, dann werden durch die Installation einer Multi-Versioning-fähigen Version zunächst alle auf der iSeries installierten Domino-Server auf den neuen Release-Stand angehoben. Dieser Schritt unterscheidet sich in der Verarbeitung nicht von den bisherigen Release-Wechseln. Allerdings werden zusätzlich die Release-spezifischen Bibliotheken (z.B. QDOMINO6xx) und Verzeichnisse (z.B. QIBM/Prodddata/Lotus/Domino6xx) angelegt.



Kopierübersicht

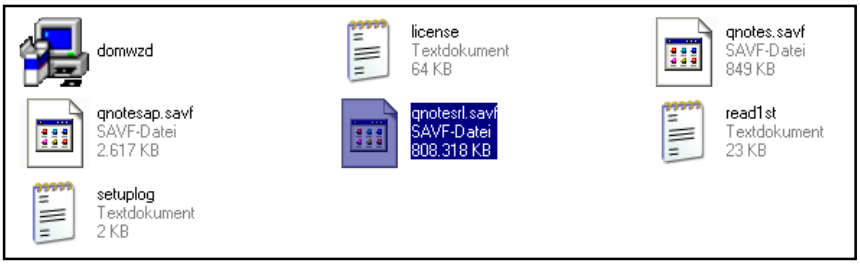
Wer über einen entsprechenden Vertrag mit Lotus oder IBM verfügt, hat die Möglichkeit, den Installationscode für Notes und Domino von den jeweiligen Web-Seiten herunterzuladen. Auf

diesem Weg können sowohl Vollversionen als auch Upgrades aus dem Internet geladen werden.

In einem solchen Fall werden in dem Download-Verzeichnis mehrere einzelne Dateien gespeichert, die für die Installation benötigt werden. Diese beinhalten neben dem eigentlichen Installationscode auch die jeweiligen Anleitungen für die Installation der Software, die Lizenzbestimmungen und den Installations-Wizard, der in Kapitel 4.2.2 im Detail beschrieben ist.

Während des Downloads werden folgende Dateien geladen:

- der Installations-Wizard „DOMWZD“
- die Lizenzbestimmungen „license“
- die Installationsanleitung „read1st“
- die „Setuplog“
- die einzelnen Sicherungsdateien für die Domino-Optionen
  - QNOTES.SAVF
  - QNOTESAP.SAVF
  - QNOTESRL.SAVF



Dateien

Nachfolgend werden zunächst die Daten der ersten Multi-Versioning-fähigen Version mittels FTP auf die iSeries übertragen. Da mit diesem Verfahren lediglich der Installationscode auf die iSeries kopiert wird, ist es unerheblich, ob auf der iSeries bereits ein Domino-Server installiert ist, das Release eines bereits vorhandenen Servers gewechselt oder eine Neuinstallation durchgeführt werden soll.

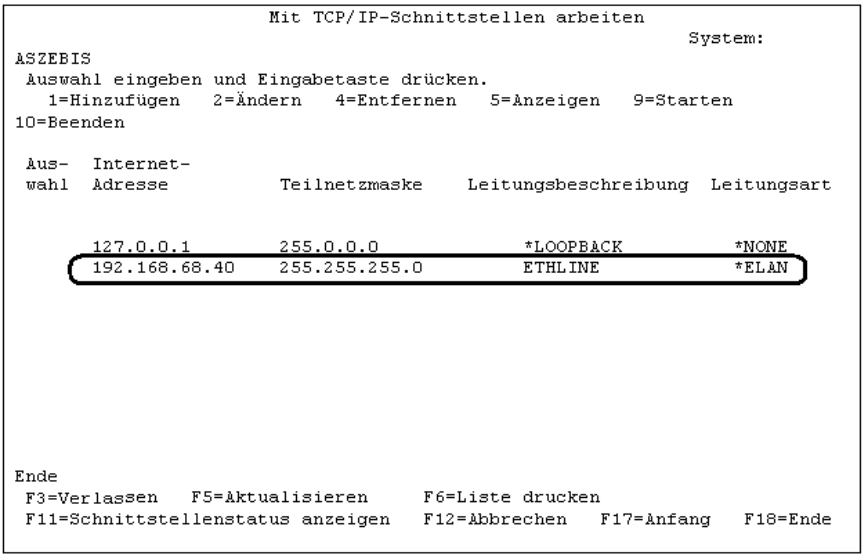
Für die Übertragung der Dateien von dem PC auf die iSeries muss entweder der Host-Name der iSeries oder deren TCP/IP-Adresse bekannt sein.

In diesem Beispiel wird mit der TCP/IP-Adresse der iSeries gearbeitet.

```
CFGTCP                          TCP/IP konfigurieren
                                                              System:
ASZEBIS
 Auswahlmöglichkeiten:

      1. Mit TCP/IP-Schnittstellen arbeiten
      2. Mit TCP/IP-Leitwegen arbeiten
      3. TCP/IP-Attribute ändern
      4. Mit TCP/IP-Port-Einschränkungen arbeiten
      5. Mit Informationen für fernes TCP/IP-System arbeiten

     10. Mit TCP/IP-Host-Tabelleneinträgen arbeiten
     11. TCP/IP-Host-Tabelle mischen
     12. TCP/IP-Domäneninformationen ändern

     20. TCP/IP-Anwendungen konfigurieren
     21. Zugehörige Tabellen konfigurieren
     22. Punkt-zu-Punkt-TCP/IP konfigurieren


 Auswahl oder Befehl
 ===>  1

 F3=Verlassen   F4=Bedienerführung   F9=Auffinden   F12=Abbrechen
```

Mit TCP/IP-Schnittstellen arbeiten

Mit der Auswahl „1“ „Mit TCP/IP Schnittstellen arbeiten“ gelangt man in die Übersicht aller definierten TCP/IP-Schnittstellen. Nun muss aus der Liste aller Schnittstellen diejenige ausgewählt werden, mit der die Kommunikation über FTP aufgebaut werden soll. In unserem Beispiel verwenden wir die Schnittstelle, die der Ethernet-Leitung zugeordnet ist. Diese erkennt man im rechten Bereich der Maske unter dem Parameter „Leitungsart“. Ethernet-Verbindungen haben hier den Eintrag „*ELAN“. Wer mit einem Token-Ring-Netzwerk arbeitet, muss an dieser Stelle den entsprechenden Eintrag für diese Leitung verwenden.



TCP/IP-Schnittstelle

Die unter dem Abschnitt „Internet-Adresse“ stehende IP-Nummer sollte nun notiert werden, denn diese wird für die Übertragung der Domino-Dateien benötigt.

Anmerkung:
Weitere Informationen zu TCP/IP im Zusammenhang mit der Domino-Installation finden Sie auch unter Kapitel 4.2.1!

Wie man schon an den Endungen der drei Dateien, die die Domino-Optionen enthalten, feststellen kann, handelt es sich um Sicherungsdateien (Savefiles) – also Container, die Sicherungsinformationen bzw. Sicherungsobjekte beinhalten.

Um diese nun von einem PC auf die iSeries übertragen zu können, muss zunächst für jede dieser Optionen auf der iSeries eine entsprechende Sicherungsdatei (SAVF) angelegt werden. Es kann zwar auch mit einer einzigen SAVF gearbeitet werden, deren Inhalt nach jeder einzelnen Optionsübertragung von dem PC auf die iSeries einzeln verarbeitet werden muss; es empfiehlt sich wegen der Übersichtlichkeit die Definition einzelner, eindeutiger Sicherungsdateien.

Die Sicherungsdateien können in jeder beliebigen Bibliothek auf der iSeries angelegt werden. In unserem Beispiel wird die Bibliothek „QGPL“ verwendet.

Mit dem Befehl „CRTSAVF“ wird für jede Option eine entsprechende Sicherungsdatei in der angegebenen Bibliothek angelegt:

```
CRTSAVF FILE(QGPL/QNOTES) TEXT('Sicherungsdatei QNOTES')
```

SAVF anlegen

Dieser Befehl wird für alle Domino-Optionen durchgeführt:

- CRTSAVF FILE(biblname/QNOTES)
- CRTSAVF FILE(biblname/QNOTESAP)
- CRTSAVF FILE(biblname/QNOTESRL)

Anmerkung:
Der Name der Sicherungsdateien ist frei wählbar und hat keine weitere Bedeutung für den Installationsprozess. In dem Beispiel wurden zum Zwecke der Zuordnung und des Verständnisses dieselben Namen verwendet, wie sie auch in der PC-Datei verwendet werden.

Nun sind alle Voraussetzungen für die Übertragung der Installationsdateien auf die iSeries gegeben.

Die Übertragung der Dateien von einem PC auf die iSeries kann auf unterschiedlichen Wegen erfolgen. Nachfolgend wird eine einfache Variante dargestellt, die mit Standardwerkzeugen auf PC-Ebene möglich ist. Dazu wird keine besondere Zusatz-Software benötigt. Grundlage für das gezeigte Beispiel ist eine Betriebssystem-Version von Microsoft. Selbstverständlich stehen ähnliche Werkzeuge auch unter Linux zur Verfügung!

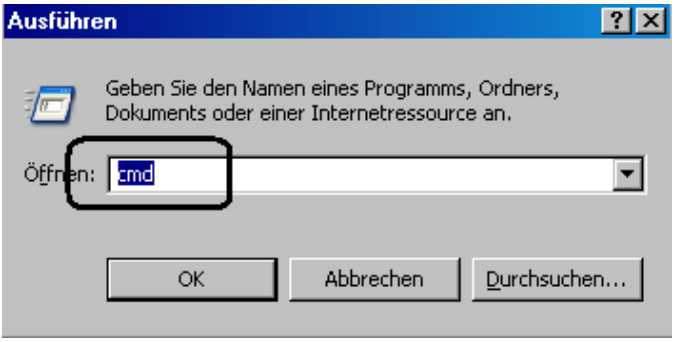
Auf dem PC, von dem die heruntergeladenen Installationsdateien auf die iSeries übertragen werden sollen, wird zunächst eine FTP-Verbindung zur iSeries hergestellt. Dazu wird auf dem PC das Befehlseingabefenster geöffnet:

Links unten in der Windows-Anzeige befindet sich die Schaltfläche „Start“ – und nach einem Klick darauf wird die Arbeitsleiste von Windows angezeigt.

Befehlsfenster starten

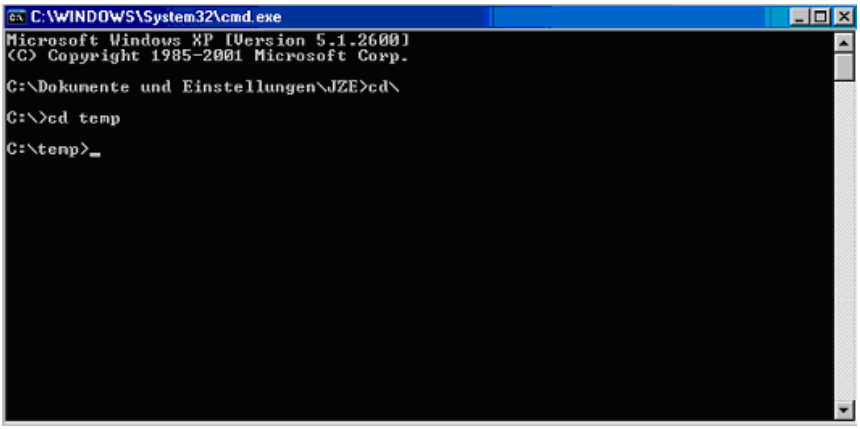
Durch einen Klick auf die Schaltfläche „Ausführen“ wird das Fenster „Ausführen“ geöffnet.

In der Eingabezeile wird nun „cmd“ eingegeben.



cmd

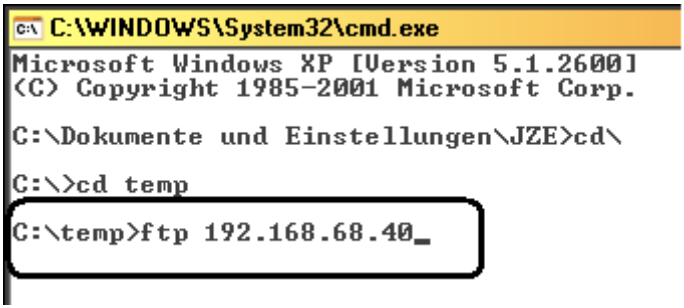
Dies ist der Befehl, der ein DOS-Eingabefenster öffnet. Nach einem Klick auf die Schaltfläche „OK“ erscheint das DOS-Eingabefenster. Zunächst wird der Pfad angegeben, in dem sich die zu übertragenden Dateien befinden. In diesem Beispiel sind die Domino Installations-Dateien in dem Verzeichnis „c:/temp“ gespeichert.



Installationspfad

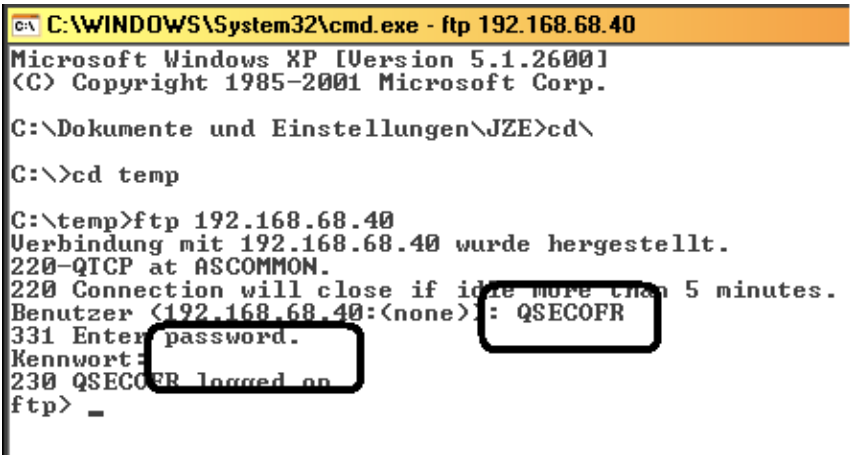
Hier kann jedes beliebige Verzeichnis angegeben werden, auf das der PC-Benutzer zugreifen kann. Auch die Übertragung der Dateien – zum Beispiel von einer CD aus – ist auf diesem Weg möglich.

Nun wird der Befehl „FTP“ gefolgt von der IP-Adresse der iSeries (oder dem Host-Namen der iSeries) in das DOS-Fenster angegeben. In dem Beispiel hat die iSeries die IP-Adresse „192.168.68.40“.



FTP IP Adresse

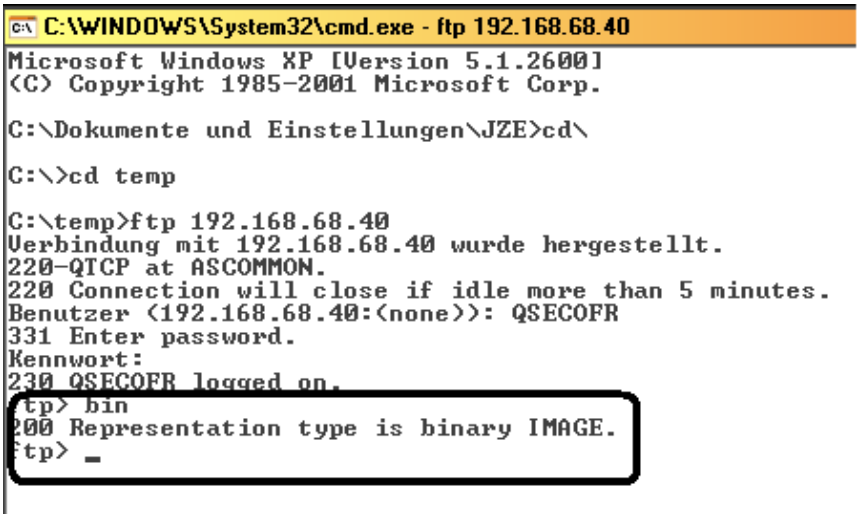
Nach der erfolgreichen Verbindung mit der iSeries werden der Benutzer und das dazugehörige Kennwort abgefragt. Hier sollte ein iSeries-Benutzer angegeben werden, der über ausreichende Berechtigungen zum Zurückspeichern der Dateien verfügt. Nachfolgend wird der Benutzer QSECOFR verwendet.



FTP-Benutzer

Ist die Anmeldung auf der iSeries erfolgreich, dann wird dies durch die Meldung „benutzername logged on“ signalisiert.

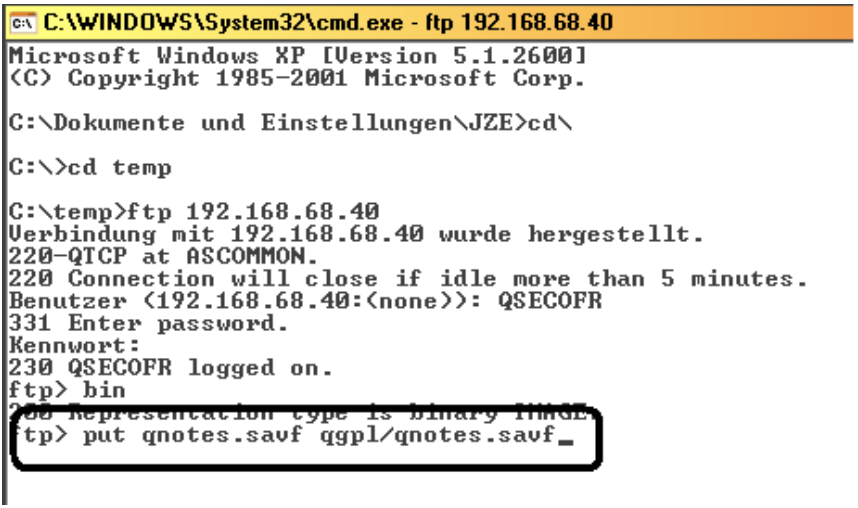
Für die Datenübertragung der Sicherungsdateien ist der Binary-Mode erforderlich, in diesen wird durch die Angabe „bin“ gewechselt.



FTP Binary

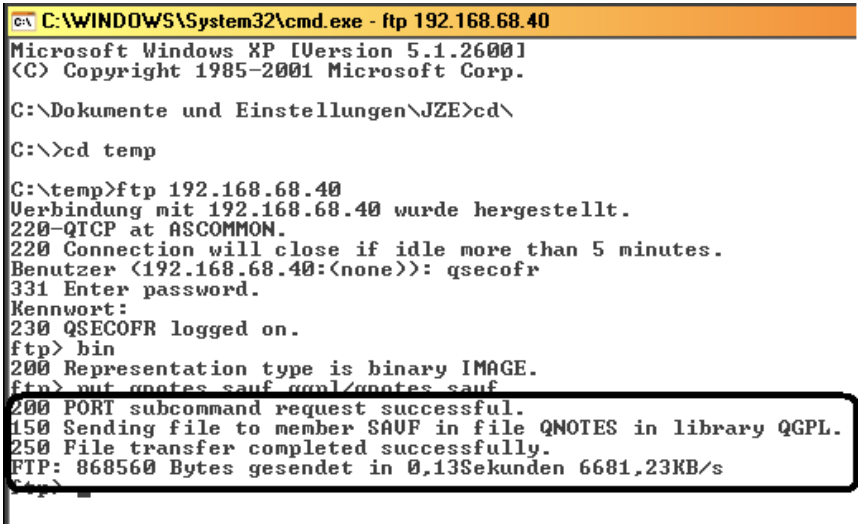
Nun wird durch den FTP-Befehl „put“ die Übertragung durchgeführt. Dieser Befehl hat den Aufbau:

Put ursprungsdatei.dateiart zielbibliothek/zieldatei.zieldateiart



FTP put

Nach der erfolgreichen Übertragung wird eine entsprechende Meldung angezeigt.



FTP-Transfer erfolgreich

Diese Übertragung muss für alle Installationsoptionen von Domino durchgeführt werden.

- QNOTES
- QNOTESAP
- QNOTESRL

Wurde für alle drei Teilbereiche die FTP-Übertragung durchgeführt, dann ist der für die Installation des Domino-Servers erforderliche Installationscode nun in den bei der FTP-Übertragung angegebenen Sicherungsdateien auf der iSeries vorhanden.

Als Nächstes folgt nun die Installation der übertragenen Domino-Software.

Es gibt, wie im vorhergehenden Kapitel eingehend beschrieben, unterschiedliche Möglichkeiten, einen Domino-Server auf der iSeries zu installieren.

Nachfolgend wird zunächst ein Domino-Server Release 6.5 unter der Verwendung des Befehls „RSTLICPGM“ installiert.

Der Installationscode wurde – wie zuvor beschrieben – in drei Sicherungsdateien innerhalb der Bibliothek QQGPL zurückgespeichert. Nun müssen die einzelnen Lizenzprogramm-Optionen, die sich aus dem Installationscode ergeben, installiert werden. Diese werden beginnend mit der Option „*BASE“ ausgeführt.

Dazu wird in der OS/400-Befehlszeile „RSTLICPGM“ eingegeben – gefolgt von der F4-Taste. Als „Produkt“ muss die Lizenzprogramm-Nummer angegeben werden. Hier ist darauf zu achten, dass die korrekte Lizenzprogramm-Nummer verwendet wird (5733-LD6 bei Domino-Release 6.0.x Versionen und 5733-L65 bei Domino-Release 6.5.x Versionen), anderenfalls schlägt die Installation fehl.

Als Installationseinheit wird in diesem Fall die Sicherungsdatei (*SAVF*)* angegeben.

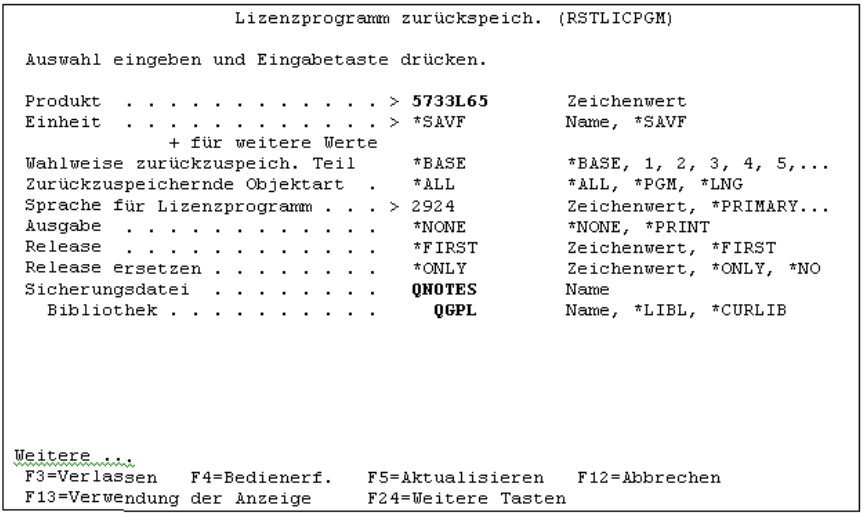
Je nach zu installierender Option muss in dem Parameterfeld „Wahlweise zurückzuspeich. Teil“ die Option angegeben werden, die sich in der Sicherungsdatei befindet (z.B. Option 10 für Domino 6.5.0).

In dem Beispiel wird die globale englische Version installiert, die durch die Sprachversion „2924“ gekennzeichnet ist.

Als Sicherungsdatei wird der Speicherort der Savefile angegeben, in unserem Beispiel war dies die „QGPL/QNOTES“ für die Option *BASE von Domino.

ACHTUNG!

Es erfolgt keine Prüfung, ob die getätigten Auswahlen in einem logischen Zusammenhang stehen. Wenn sich in der Sicherungsdatei “QGPL/QNOTES” nicht die erwartete Option *BASE befindet, wird die Rücksicherung mit einem Fehler abbrechen.



RSTLICPGM

4.2.4.2.2 Installation Multi-Versioning Release 2

Ist auf einer iSeries innerhalb einer Partition ein Multi-Versioning-fähiges Release installiert, können weitere Multi-Versioning-fähige Release-Versionen parallel eingerichtet werden. Dabei werden Release-spezifische Informationen in den dafür vorgesehenen Bibliotheken und Verzeichnissen gespeichert. Bei jeder Installation eines Multi-Versioning-fähigen Release-Standes wird geprüft, ob dieser das Primary-Release ist und die Release-unabhängigen Domino-Objekte liefert.

Soll das Multi-Versioning-Release zusätzlich auf der iSeries installiert werden und sind die bereits installierten Server von dieser Installation nicht betroffen (das heißt, es wird kein Release-Wechsel auf bereits installierten Servern durchgeführt), dann können die installierten Server während des Installationsprozesses aktiv bleiben und müssen nicht – wie bei einem Server-Upgrade – beendet werden.

Die zweite Domino Release-Version – in diesem Beispiel das Release 6.0.3 – wird unter Verwendung der Installationsmethode „LODRUN“ eingerichtet.

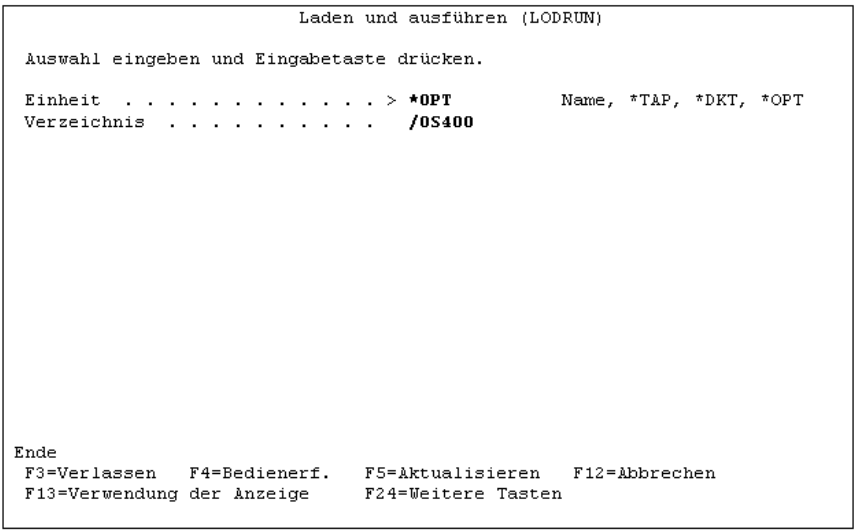
Die Voraussetzungen des iSeries-Systems bezüglich der erforderlichen Lizenzprogramme und des notwendigen PTF-Standes werden in diesem Beispiel als gegeben angenommen. Die Installation wird mit einem Benutzerprofil durchgeführt, das über ausreichende Berechtigungen verfügt – nachfolgend wird der Benutzer „QSECOFR“ für die Installation verwendet.

Für die Installation des Domino-Servers mit dem Befehl „LODUN“ ist die für die Installation erforderliche Installations-CD in das dafür vorgesehen Laufwerk der iSeries einzulegen.

Für die Installation eines Domino 6.0.3 Servers sind zwei CDs notwendig, die die Bezeichnung „Lotus Domino for iSeries OS/400 V5R1, OS/400 V5R2“ tragen. Ist die Software auf einem anderen Medium vorhanden, dann kann dieses natürlich auch verwendet werden. In einem solchen Fall sind die Angaben für die Installationsquelle der nachfolgenden Befehle entsprechend anzupassen.

Die Anzahl der erforderlichen Installations-CDs variiert mit den einzelnen Release-Versionen.

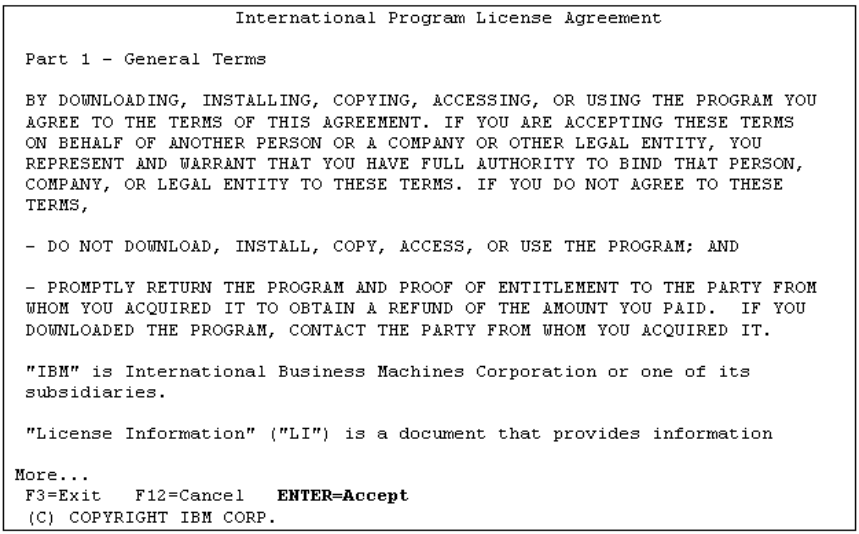
Nach dem Einlegen der ersten CD in das Laufwerk wird in der Befehlszeile des Bildschirms der Befehl „LODRUN“ qualifiziert oder unter Verwendung der Befehlserweiterungs-Funktionstaste „F4“ eingegeben.



LODRUN

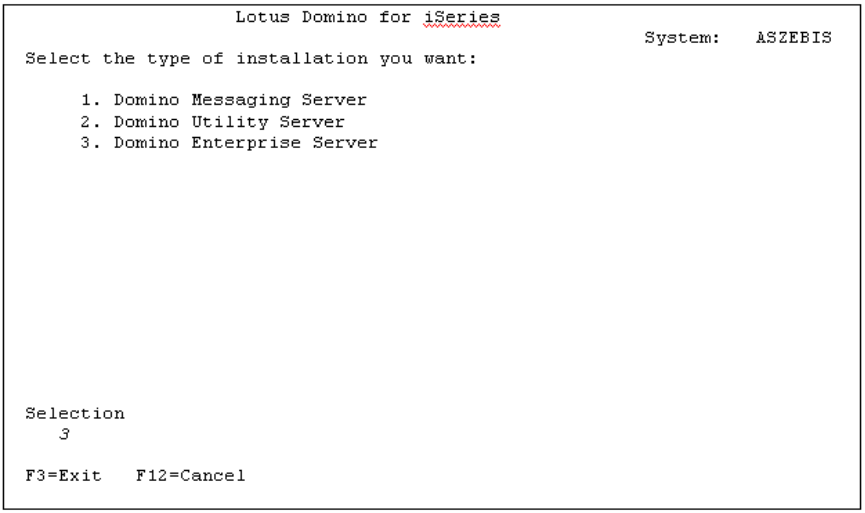
Bei Verwendung einer Installations-CD ist der Parameter „Einheit“ mit „*OPT“ zu füllen. Das Verzeichnis, in dem sich die Installationsdaten auf der CD befinden, lautet „OS400“ und ist mit einem führenden „/“ (Slash) einzugeben.

Nach dem Drücken der Datenfreigabetaste beginnt die Installation. Als Erstes werden die Lizenzbestimmungen angezeigt, die zunächst durch eine Bestätigung mit der „Enter“-Taste akzeptiert werden müssen.



Lizenzbestimmungen

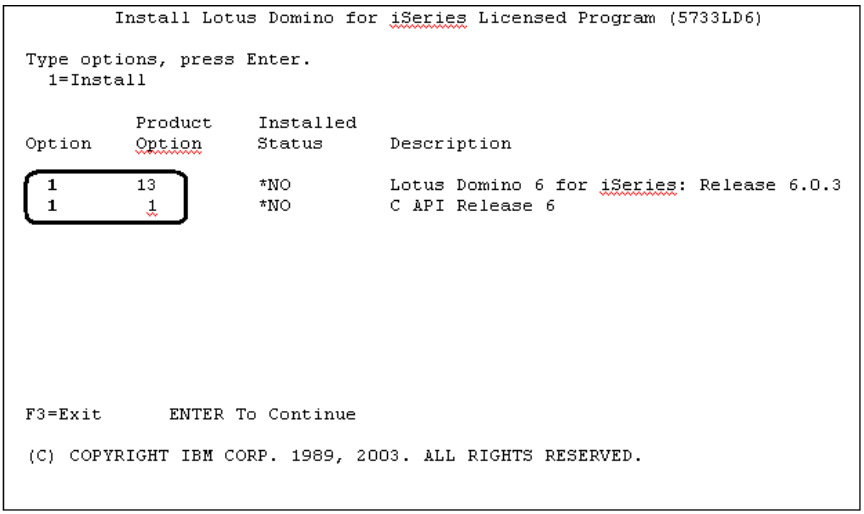
Der Domino-Server besteht – und das auch lizenzrechtlich – aus verschiedenen Server-Typen. Der gewünschte Server ist in der nächsten Anzeige anzugeben. Details über den Funktionsumfang der unterschiedlichen Server-Typen finden Sie in den vorhergehenden Kapiteln.



Server-Typ

In diesem Beispiel wird ein Domino Enterprise Server installiert.

Wie bereits weiter oben in diesem Kapitel beschrieben, besteht die Installation des Domino-Servers auf einer iSeries aus unterschiedlichen Optionen. Diese werden nun zur Auswahl für die Installation vorgeschlagen.



Optionsauswahl

Jede zu installierende Option muss in der nachfolgenden Anzeige mit einer „1“ ausgewählt werden. Die Auswahl wird dann durch die „Enter“-Taste bestätigt und die Installation danach fortgesetzt.

Anmerkung:
Bei der Verwendung des Befehls „LODRUN“ wird die Installation der Option „*BASE“ automatisch vorgenommen und in dem Installationsfenster auch nicht zur Auswahl vorgeschlagen. Wird als Installationsverfahren dagegen „RSTLICPGM“ verwendet, dann ist zu beachten, dass die Option „*BASE“ nur unter bestimmten Voraussetzungen installiert werden sollte.

Der nächste Schritt kann je nach iSeries unterschiedlich lange laufen. Es folgt nun das Kopieren und anschließende Entpacken der Installationsdaten von der CD auf die Platte der iSeries. Der Installationsfortschritt wird durch eine Nachricht am unteren Bildschirmbereich angezeigt.

```
Uncompressing option 13. This may take a while, please be patient.
```

Entpacken

Nach dem Entpacken wird die Software installiert. Dies wird ebenfalls durch eine Statusanzeige mitgeteilt.

```
Installing option 13 ...
```

Installieren

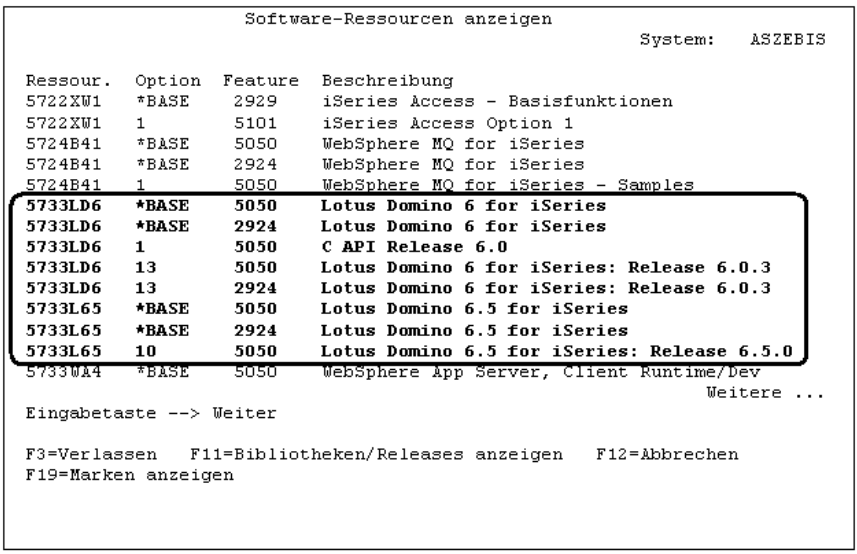
Nach Beendigung des Kopierens des Installationscodes wird eine Nachricht ausgegeben, die im Falle einer erfolgreichen Installation wie folgt aussehen sollte:

```
Command LODRUN ended successfully.
```

Erfolgsmeldung

Sollte während der Installation ein Fehler auftreten, dann kann in dem Joblog nachgesehen werden, aus welchem Grund die Installation fehlgeschlagen ist. Dazu wird der Befehl „DSPJOBLOG“ in der OS/400-Befehlszeile eingegeben.

Der Abschluss der Installation der Domino-Software kann mit dem Befehl „DSPSFWRSC“ kontrolliert werden. In der Anzeige sollten sich die ausgewählten Optionen befinden. Entgegen der Anzeige der installierten Lizenzprogramme werden in der Anzeige der Software-Ressourcen auch die Details der einzelnen Features aufgelistet. Neben den Basis-Features werden auch die sprachspezifischen Features angezeigt. In dem Beispiel wurde ein englischer Server installiert, der durch den Feature Code „2924“ dargestellt wird. Wird das entsprechende deutsche Sprachpaket installiert, dann erscheint dieses mit dem Feature-Code „2929“.

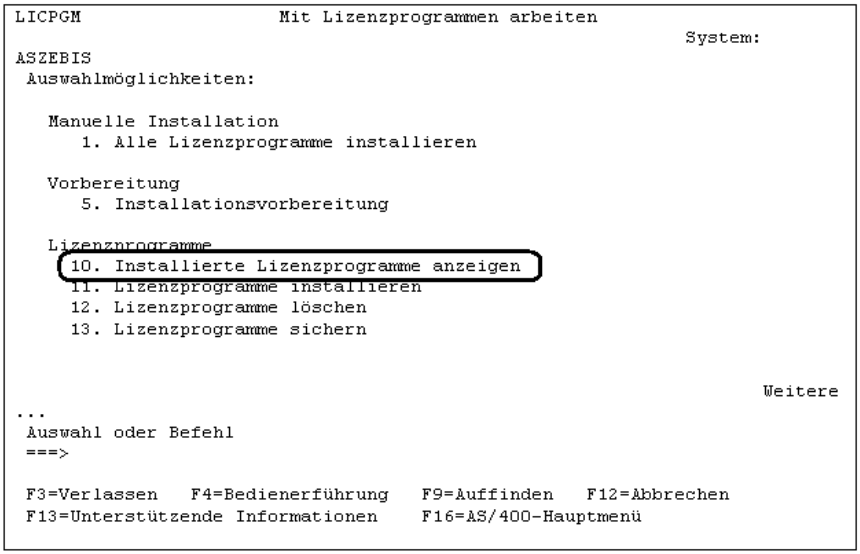


```
                    Software-Ressourcen anzeigen
                                                          System:   ASZEBIS

Ressour.  Option  Feature  Beschreibung
5722XW1   *BASE    2929     iSeries Access - Basisfunktionen
5722XW1   1         5101     iSeries Access Option 1
5724B41   *BASE    5050     WebSphere MQ for iSeries
5724B41   *BASE    2924     WebSphere MQ for iSeries
5724B41   1         5050     WebSphere MQ for iSeries - Samples
5733LD6   *BASE    5050     Lotus Domino 6 for iSeries
5733LD6   *BASE    2924     Lotus Domino 6 for iSeries
5733LD6   1         5050     C API Release 6.0
5733LD6   13        5050     Lotus Domino 6 for iSeries: Release 6.0.3
5733LD6   13        2924     Lotus Domino 6 for iSeries: Release 6.0.3
5733L65   *BASE    5050     Lotus Domino 6.5 for iSeries
5733L65   *BASE    2924     Lotus Domino 6.5 for iSeries
5733L65   10        5050     Lotus Domino 6.5 for iSeries: Release 6.5.0
5733WA4   *BASE    5050     WebSphere App Server, Client Runtime/Dev
                                                                Weitere ...
Eingabetaste --> Weiter

F3=Verlassen   F11=Bibliotheken/Releases anzeigen   F12=Abbrechen
F19=Marken anzeigen
```

DSPSFWRSC

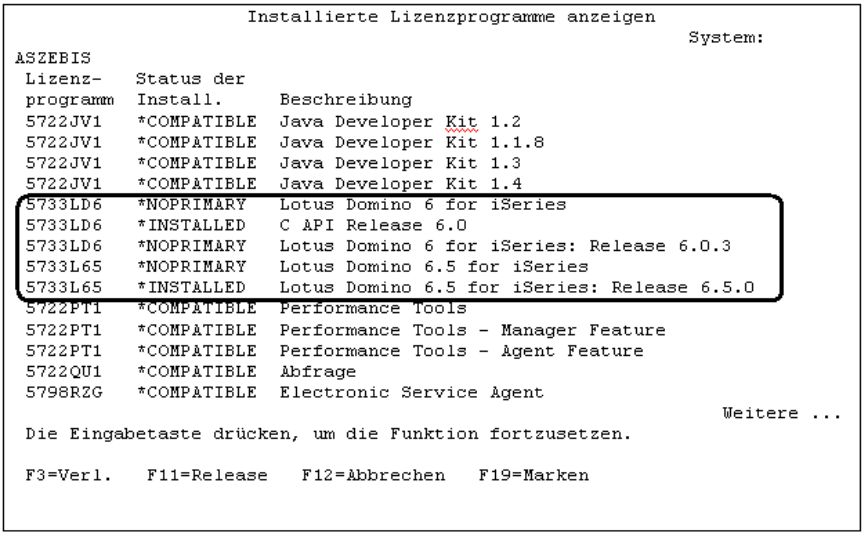
Die Option „1“ (C-API) ist nur einfach vorhanden. Genau genommen ist die Option 1 nicht Multi-Versioning-fähig. Sie wird mit dem Primary-Release installiert beziehungsweise ersetzt.

Alternativ kann zur Überprüfung der Installation auch das Menü „Mit Lizenzprogrammen arbeiten“ genutzt werden. Dazu wird zunächst in der Befehlszeile der Befehl „GO LICPGM“ eingegeben, mit dem dann in dieses Menü verzweigt wird.



GO LICPGM

Die Auswahl „10“ zeigt alle auf der iSeries installierten Lizenzprogramme einschließlich der Lizenzprogramme für Domino an. Nach mehrmaligem Blättern erscheinen die Einträge für Domino:



Lizenzprogramme anzeigen

Der Status der einzelnen Domino-Komponenten sollte entweder „NOPRIMARY“ oder „INSTALLED“ haben. Es kann vorkommen, dass die Installation eines Lizenzprogramms fehlschlägt. In einem solchen Fall würde der Status „*ERROR“ für diese Option erscheinen und das Lizenzprogramm muss erneut installiert werden.

Nach dem Abschluss der Installation mehrerer Multi-Versioning-fähiger Release-Versionen befinden sich die dazugehörigen Objekte mehrfach in den jeweiligen Bibliotheken auf dem System.

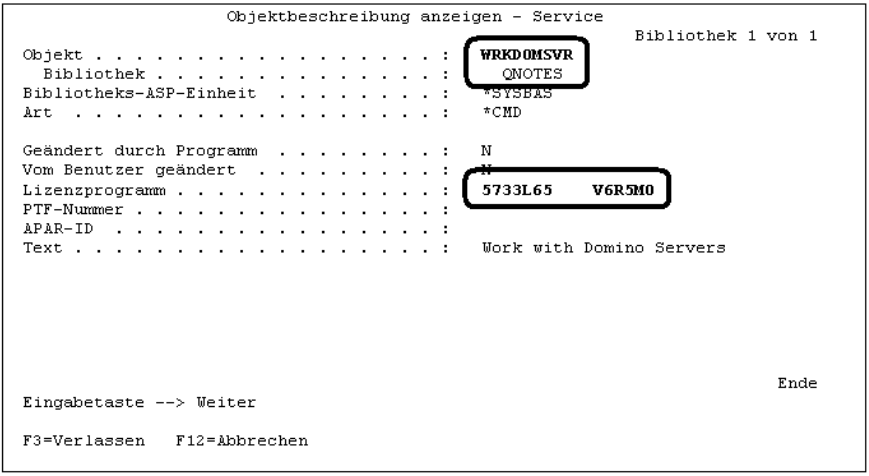
So befindet sich zum Beispiel der Befehl „WRKDOMSVR“ in den Bibliotheken

- QNOTES
- QDOMINO603
- QDOMINO650

Bedingt durch die Prüfung auf das „Primary Domino Release“ wird während des Installationsprozesses die aktuellsten Objektversionen in die allgemeinen Release-unabhängigen Bibliotheken gespeichert.

Bei der in dem Beispiel verwendeten Konstellation ist das Release 6.5.0 das höhere und wurde als „Primary Release“ festgelegt. Somit befinden sich in den Bibliotheken QSYS und QNOTES auch die Objekte aus der Bibliothek QDOMINO650.

Die nachfolgende Anzeige soll dies verdeutlichen. Sie enthält die Objektbeschreibung des Befehls „WRKDOMSVR“ aus der Domino Release-unabhängigen Bibliothek QNOTES. In dem Parameter „Lizenzprogramm“ befindet sich die Herkunft des Befehls.



Objektversion

Anmerkung:

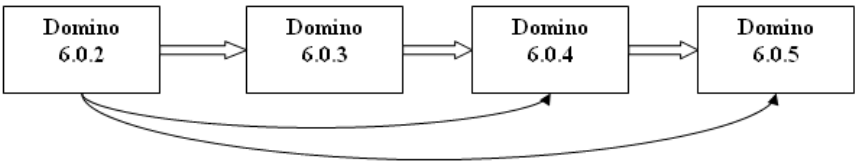
Es kann durchaus vorkommen, dass ein neu zu installierendes Domino-Release nicht als Primary-Release verwendet wird, wenn die Objekte eines bereits vorhandenen Release die Unterstützung aller Domino-Versionen gewährleistet.

4.2.4.3 Migration Multi-Versioning Server

Ist auf einer iSeries bereits ein Multi-Versioning Release installiert, dann unterscheidet sich der Installations- oder Migrationsprozess von den bisherigen Release-Wechseln. Denn bei der Installation der Domino-Software kann oder muss angegeben werden, ob diese zusätzlich zu der bereits vorhandenen Software installiert werden soll oder ob die vorhandene Software-Version migriert werden soll. Zudem bestehen besondere Abhängigkeiten durch die unterschiedlichen Lizenzprogramm-Versionen, die bei einer Migration beachtet werden müssen.

4.2.4.3.1 Migration Domino 6.0.x Server

Soll ein Domino-Server mit dem Release-Stand 6.0.x. (Lizenzprogramm-Nummer 5733-LD6) migriert werden, dann kann dies direkt auf das nächst höhere Release innerhalb dieser Produktgruppe (5733-LD6) erfolgen. Es können aber auch einzelne Release-Versionen übersprungen werden. Informationen, welche Upgrade-Pfade bei den jeweiligen Release-Ständen unterstützt werden, sollten vor jedem Release-Wechsel genau geklärt werden, um Abbrüche während der Migration zu vermeiden.

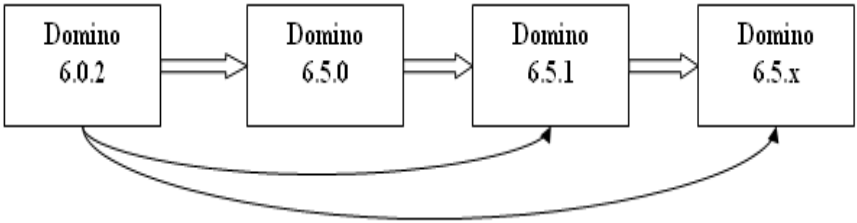


Upgradepfad 60x

Ist auf einem System das nicht Multi-Versioning-fähige Release (!) 6.0.2 installiert, dann kann eine Migration auf die Release-Version 6.03 oder direkt auf die Release-Version 6.0.4 erfolgen.

4.2.4.3.2 Migration Domino 6.5.x Server

Das Release-Wechsel-Verfahren bei einem Domino 6.5.x Server (Lizenzprogramm Nr. 5733-L65) unterscheidet sich bezüglich der Anforderungen und der Upgrade-Möglichkeiten nicht von der zuvor für die Versionen 6.0.x beschriebenen Variante. Auch hier gilt, dass der jeweilige Upgrade-Pfad auf jeden Fall vor der Installation geprüft werden muss. Die Lizenznummern der einzelnen Release-Versionen bleiben in jedem Fall gleich.

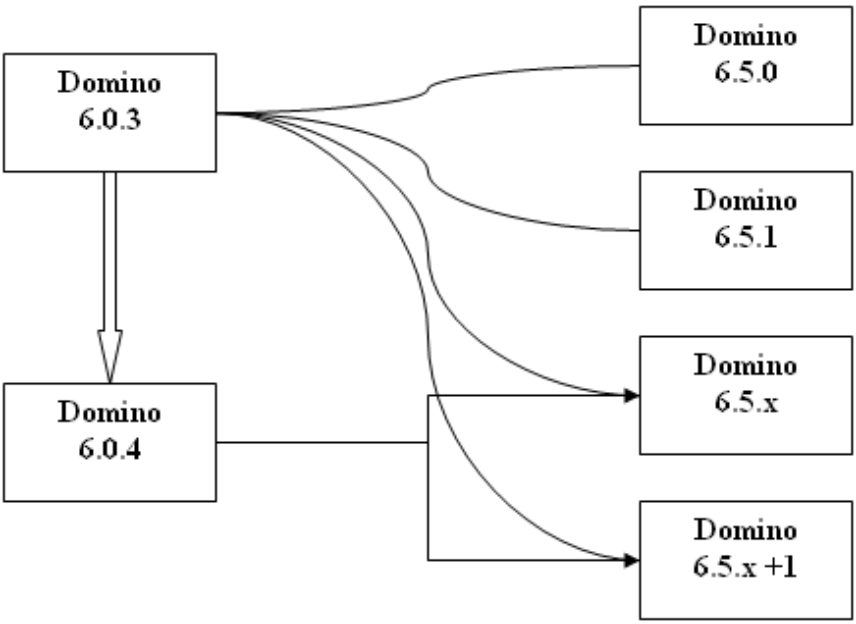


Upgradepfad 65x

4.2.4.3.3 Migration Domino 6.0.x nach 6.5.x

Vor einem Release-Wechsel von einer Domino 6.0.x Version (5733-LD6) auf ein Domino 6.5.x Release (5733-L65) ist es wichtig, zu klären, welche der beiden Versionen den höheren Release-Level besitzt.

Innerhalb der beiden Produktgruppen 5733-LN6 und 5733-L65 können durchaus unterschiedliche Release-Level vorhanden sein; die Versionsnummer 6.0.x bzw. 6.5.x sagt nichts in Bezug auf den Release-Level der beiden Produkte untereinander aus. Die nachfolgende Grafik verdeutlicht, welche Migrations-Möglichkeiten der beiden Produkte derzeit zur Verfügung stehen.



Upgrademöglichkeiten

Nach dieser Grafik ist kein Wechsel von einer Domino 6.0.4 Version auf eine Version 6.5.0 oder 6.5.1 möglich, da dies genau genommen ein Downgrade wäre und es dafür keinen vorgesehenen Pfad gibt.

4.2.5 Domino-Performance auf iSeries

Domino auf iSeries bedeutet für die Integration und auch für die Konfiguration der iSeries einige wichtige Aspekte, die unbedingt im Vorfeld der Installation beziehungsweise bei der Anschaffung eines iSeries-Modells abgeklärt werden müssen.

Außer durch korrektes Sizing der Hardware sind auch auf einer gut ausgerüsteten Maschine durch geschickte Einstellungen der Systemwerte und einiger anderer performance-beeinflussender Werte oft wesentlich bessere Leistungsdaten für Domino und zum Teil auch für die gesamte iSeries zu erreichen.

In dem nachfolgenden Abschnitt wird deshalb explizit auf das Thema „Performance von Domino auf iSeries“ eingegangen.

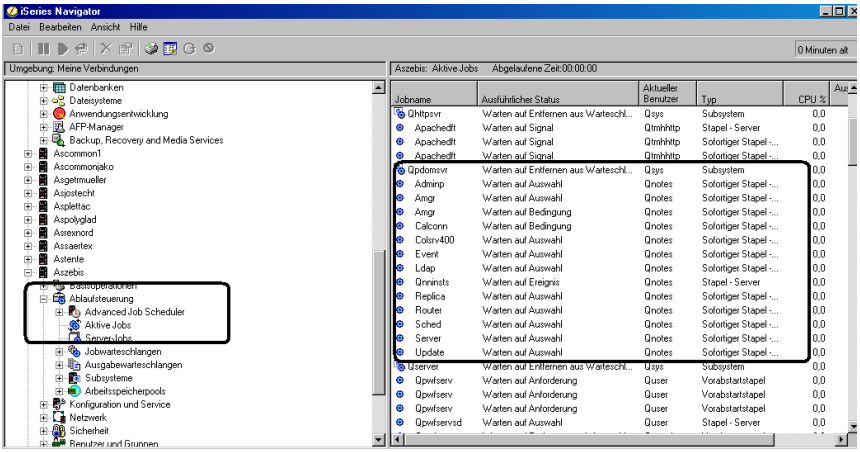
Dabei ist es wichtig, dass für das optimale Zusammenspiel der beiden Produkte „Domino“ und „iSeries“ Einstellungen auf beiden Seiten notwendig sind. Leider sind die optimalen Systemeinstellungen nicht immer per Default gegeben.

Für Domino gilt, wie für viele andere Applikationen auch, dass die einzelnen Teilbereiche in den beiden Leistungsbereichen der iSeries – dem interaktiven Bereich und dem Batch-Bereich – ausgeführt werden können. Die Beeinflussung dieser beiden Bereiche kann getrennt vorgenommen werden. Wichtig ist dabei, dass die interaktive Leistung bei einigen iSeries-Modellen durch das interaktive Feature bestimmt wird. Ist dieses Feature zu klein ausgelegt, dann kann dies zu Geschwindigkeitsproblemen führen.

Die nachfolgende Tabelle gibt einen Überblick über die Standard-Tasks eines Domino Servers sowie über die Bereiche, in denen diese Tasks ausgeführt werden.

Task	**Ausführungsbereich**
Mail Router	Batch
Replikationen	Batch
AdminP	Batch
Events und Reporting	Batch
One Updater (Indexing)	Interaktiv
Kalender und Schedule	Interaktiv
Agent Manager	Interaktiv

Die Jobs des Domino-Servers können mit Hilfe des iSeries Navigators oder natürlich auch mit dem OS/400-Befehl WRKACTJOB angezeigt werden. Beachten Sie die Anzahl der aktiven Jobs innerhalb des jeweiligen Domino-Subsystems. Denn diese sind durchaus indirekt Performance-beeinflussend. Welche Bedeutung dies hat, wird im weiteren Verlauf dieses Kapitels eingehender beschrieben.



Jobs

Jobsteuerung

Ein Job, der auf der iSeries ausgeführt wird, hat einige Einstellungsparameter. Über diese kann angegeben werden, wie der Job behandelt wird. Wichtige Einstellungsmöglichkeiten sind im Hinblick auf die Ausführungsgeschwindigkeit:

- Ausführungspriorität (RUNPTY)
- Zeitscheibe (TIMESLICE)
- Purge (PURGE)
- Max. Wartezeit (DFTWAIT)
- Max. Prozessorzeit (CPUTIME)
- Max. temp. Speicher (MAXTMPSTG)
- Max. Threads

RUNPTY

Die Ausführungspriorität gibt an, mit welcher Priorität ein Job im Vergleich zu anderen Jobs behandelt wird. Die Wertigkeit dieses Parameters kann zwischen 0 (hoch) und 99 (niedrig) angegeben werden.

Per Default werden einige Domino-Jobs mit der Priorität 20 ausgeführt – derselben Priorität wie etwa interaktive Jobs auch.

TIMESLICE

Die Zeitscheibe gibt an, welche Prozessorzeit einem Job (oder besser einem Thread) zugeordnet wird. Wenn ein Thread nicht in der zur Verfügung stehenden Zeit abgearbeitet werden konnte, dann können nachfolgende Situationen auftreten:

- Wenn keine weiteren Threads mit gleicher oder höherer Priorität ausgeführt werden sollen, dann wird dem Job automatisch eine andere (bessere) TIMESLICE zugeordnet und der Job bleibt für die weitere Verarbeitung im Hauptspeicher geladen und wird weiter verarbeitet.

- Wenn weitere Threads mit gleicher oder höherer Priorität ausgeführt werden, dann wird der Thread aus dem Hauptspeicher ausgelagert und in einen Wartezustand versetzt. Nachdem die anderen Threads in der ihnen zugeordneten Zeit bearbeitet wurden, wird der Job wieder in den Hauptspeicher geladen.

Der Mindestwert für diesen Parameter liegt bei 8 Millisekunden.

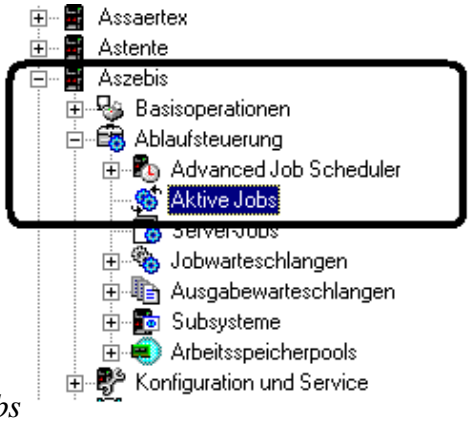
DFTWAIT

Die Standardwartezeit gibt die maximale Wartezeit an, die ein Thread im Job auf eine Systemanweisung wartet, bevor er auf Systemressourcen zugreift.

All diese Systemwerte können einen wesentlichen Einfluss auf die gesamte Leistung der iSeries haben. Die Administration dieser Parameter hat IBM im iSeries Navigator sinnvoll zusammengefasst. In vielen Bereichen favorisiert IBM den Einsatz des iSeries Navigators. In Zukunft werden wohl immer mehr Funktionen allein über dieses Tool administrierbar sein. Deshalb wird an dieser Stelle auf die Anpassung der Performance-relevanten Job-Parameter mit Hilfe des iSeries Navigators verwiesen.

Die Parameter befinden sich für jeden Job innerhalb der Ablaufsteuerung des iSeries Navigators.

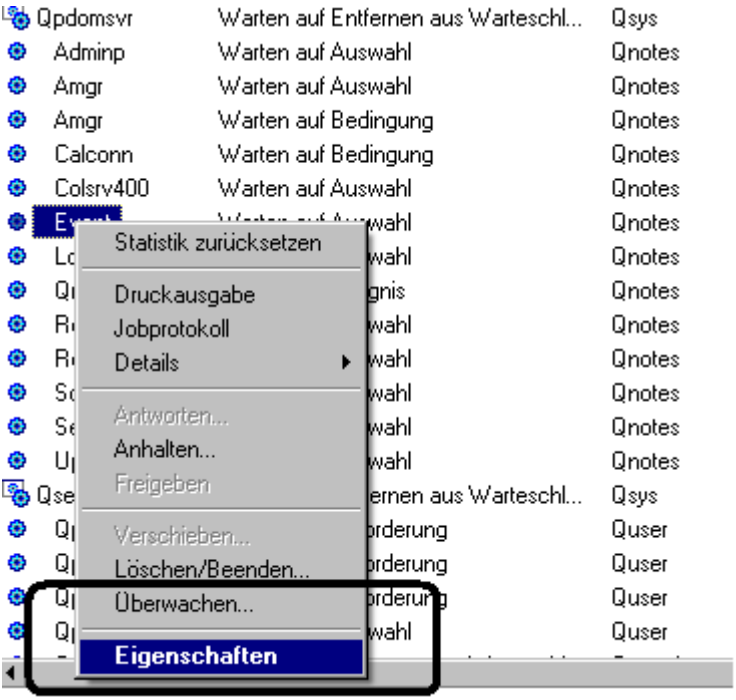
- Um diese zu nutzen, wird zunächst im linken Bereich der Anzeige des iSeries Navigators das zu verwaltende System ausgewählt.
- Dann wird der Bereich „Ablaufsteuerung“ erweitert.
  Es erscheint eine weitere Ebene, u. a. die aktiven Jobs. Diese werden durch einen Doppelklick ausgewählt.



Aktive Jobs

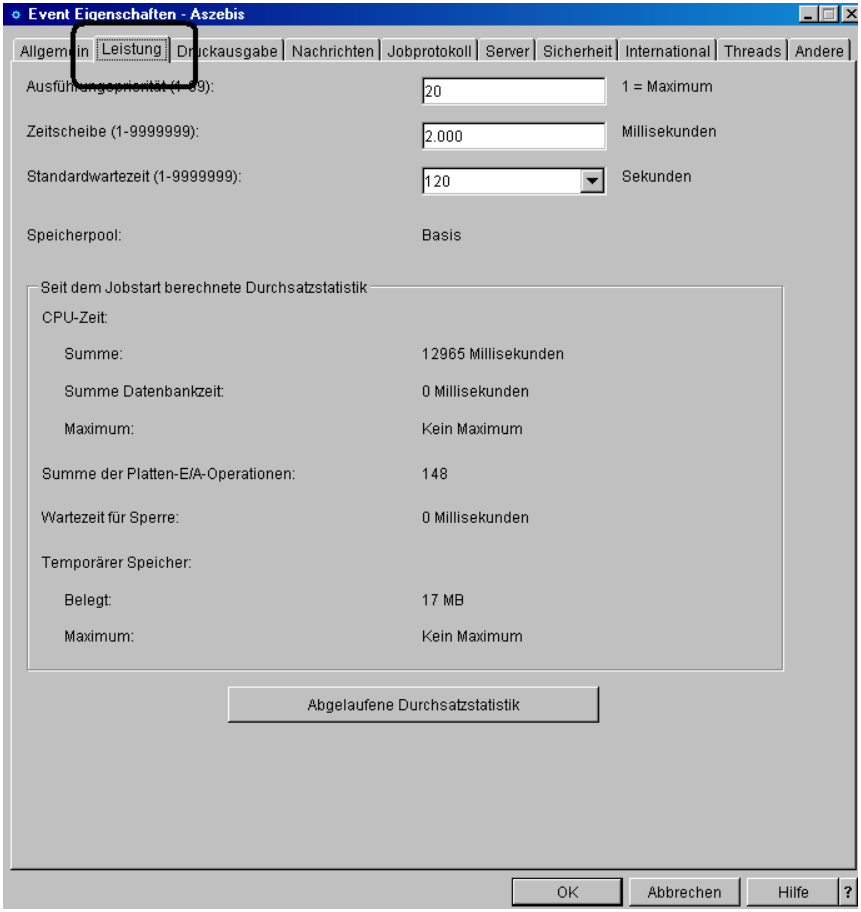
In der rechten Anzeigeseite werden die aktiven Jobs der iSeries aufgelistet, u. a. auch die unter dem Subsystem des Domino-Servers befindlichen Jobs. Diese können hier verwaltet werden.

Dazu wird die rechte Maustaste betätigt und ein Arbeitsfenster geöffnet. Eine der Auswahlmöglichkeiten sind die „Eigenschaften“ des Jobs, die nun selektiert werden.



Eigenschaften

Die Parametereinstellungen können innerhalb der Schaltfläche „Leistung“ angegeben werden:

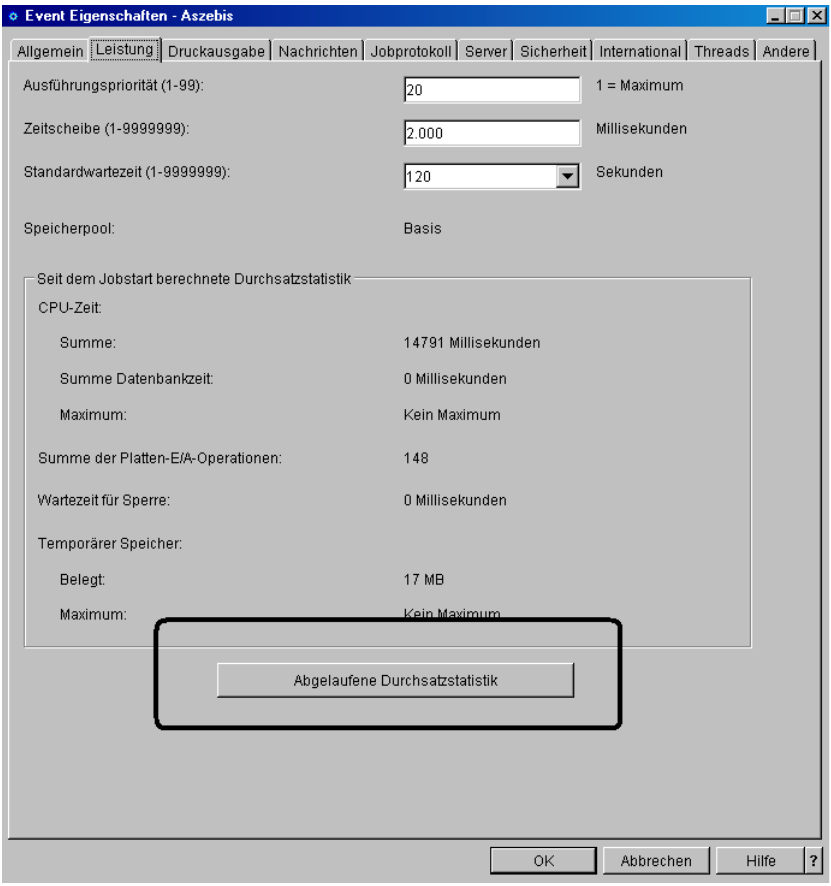


Leistung

Mit dem iSeries Navigator können die Leistungsdaten eines Jobs sehr elegant visualisiert werden. Sollte es zu Engpässen auf dem

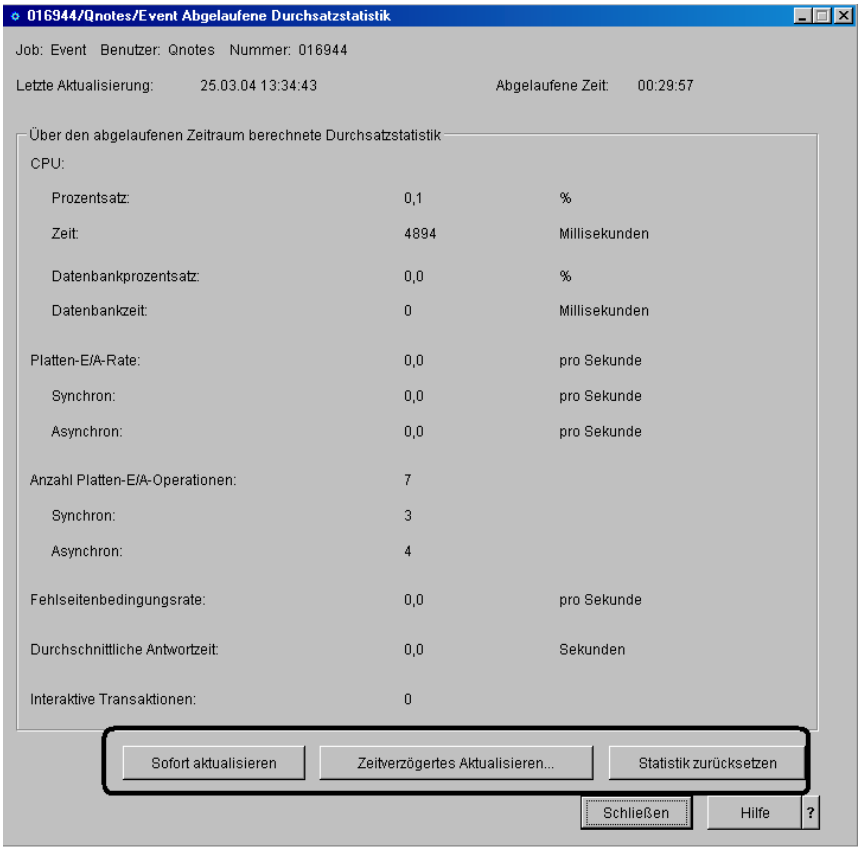
System kommen (und das nicht nur im Bereich von Domino auf iSeries), dann bietet der iSeries Navigator eine gute Möglichkeit, die Leistungsdaten des Systems zu erfassen.

Statistische Informationen findet man direkt unter der Schaltfläche „Leistung“. Unter anderem werden die CPU-Zeiten und die Plattenzugriffe angezeigt.



Durchsatzstatistik

Zusätzliche Informationen und sinnvollerweise auch solche, die für die Optimierung von Domino sinnvoll sind, können unter der Auswahl „Abgelaufene Durchsatzstatistik“ ausgewertet werden. Hier ist eine zeitgesteuerte Aktualisierung der Informationen möglich oder eine manuelle Aktualisierung, die in etwa der Funktionstaste F5 unter WRKACTJOB gleichkommt.



Abgelaufene Durchsatzstatistik

Die zuvor beschriebenen Parameter können nur temporär für einen Job geändert werden. Nach einem Systemneustart oder einem Server-Neustart werden die globalen Voreinstellungen wieder zugrunde gelegt. Sie müssten wieder manuell angepasst werden. Um die Leistungsdaten permanent anzupassen, müssen andere Lösungswege angewendet werden. Diese werden im Nachfolgenden beschrieben.

Die iSeries bietet „von Haus aus“ einige Einstellungen, die die Performance-Daten der Maschine automatisch optimal einstellen (sollen).

In der Regel wird empfohlen, den Systemwert „QPFRADJ“ (das ist der Performance-“Tuner“ der iSeries) auf automatische Anpassung (Systemwert „2“ oder „3“) einzustellen. Wird Domino auf der iSeries eingesetzt, sollte dieser Systemwert auf „3“ stehen.

4.2.5.1 Domino-Ausführungsumgebung

Leider ist dieser Systemwert nicht für alle Teilbereiche des OS/400 – oder besser für die nicht primären OS/400-Funktionen wie Domino – wirksam. Damit auch für solche Teilbereiche wie Domino optimale Leistungen erzielt werden können, muss ein die automatischen Optimierung ergänzendes Verfahren angewendet werden.

Werden keine Angaben gemacht, in welchem Pool Domino laufen soll, so werden die Default-Einstellungen der IBM übernommen. Nachteil ist, dass die automatischen Leistungsanpassungen dann in der Regel nicht greifen.

Es empfiehlt sich an dieser Stelle, Domino entweder

- in einem eigenen privaten Pool laufen zu lassen oder
- im *BASE-Pool laufen zu lassen.

Private Pool

Wird Domino in einem eigenen „Private Pool“ ausgeführt, dann können die Leistungseinstellungen für diesen Pool fest angegeben werden, ohne dass der automatische Anpassungslauf diese angreift bzw. Ressourcen von diesem Pool abzieht. Damit ist eine relativ genaue und situationsbezogene Leistungseinstellung für Domino möglich.

***BASE Pool**

QPFRADJ bedient sich bei der Leistungsanpassung auch der Ressourcen, die dem *BASE-Pool zugeordnet sind. Durch einen weiteren Systemwert – QBASPOOL – werden dessen Mindest-Hauptspeicherzuordnungen festgelegt, die durch den Systemwert QPFRADJ nicht unterschritten werden können. Durch eine geschickte Zuordnung von Hauptspeicher im Systemwert QBASPOOL ist also eine sinnvolle Performance-Einstellung für Domino möglich.

Shared Pool

Domino kann auch in einem so genannten „Shared Pool“ ausgeführt werden. Mit dem Befehl WRKSHRPOOL kann dem Domino-Server ein Minimum an Hauptspeicher zugewiesen werden.

Im nachfolgenden Beispiel wird der Domino-Server in dem Shared Pool 1 (*SHRPOOL1) ausgeführt. Bei der Definition dieses Pools wurde festgelegt, dass dieser über mindestens 800 MB Hauptspeicher verfügt. Die Festlegung des Mindesthauptspeichers erfolgt über eine Prozentangabe, die sich auf den gesamten Hauptspeicher der iSeries bezieht.

Zunächst wird der Shared Pool unter Verwendung des Befehls WRKSHRPOOL angegeben:

```
                        Mit gemeinsamen Pools arbeiten
                                                              System:   ASZEBIS
Hauptspeichergröße (M) . :        4021,40

Änderungen (falls zulässig) eingeben und die Eingabetaste drücken.

            Definierte   Max.  Zugeordn.   Pool  -Paging-Angabe-
Pool         Größe (M)  Aktiv  Größe (M)    ID   Defin.  Aktuell
*MACHINE        231,04  +++++      231,04    1   *FIXED  *FIXED
*BASE          1673,93     79     1673,93    2   *FIXED  *FIXED
*INTERACT      2116,17    185     2116,17    3   *FIXED  *FIXED
*SPOOL            0,25      1        0,25    4   *FIXED  *FIXED
*SHRPOOL1       800,00      2                    *FIXED
*SHRPOOL2         0,00      0                    *FIXED
*SHRPOOL3         0,00      0                    *FIXED
*SHRPOOL4         0,00      0                    *FIXED
*SHRPOOL5         0,00      0                    *FIXED
*SHRPOOL6         0,00      0                    *FIXED
                                                                  Weitere ...
Befehl
===>
F3=Verlassen   F4=Bedienerführung   F5=Aktualisieren   F9=Auffinden
F11=Optimierungsdaten anzeigen      F12=Abbrechen
```

Mit Pools arbeiten

Anschließend wird die Subsystembeschreibung dahingehend geändert, dass Domino in diesem neuen Pool ausgeführt wird:

CHGSBSD SBSD(QUSRNOTES/DOMINO03) POOLS((1 *SHRPOOL1))

Diese Änderung kann durchgeführt werden, während der Domino-Server läuft; sie wirkt sich allerdings erst nach einem Neustart des Domino-Servers aus.

Oftmals kommt es beim Ausführen von Domino-Jobs auf der iSeries zu Laufzeitproblemen, die die gesamte Installation beeinflussen. Besonders dann, wenn:

- einzelne Domino-Jobs eine hohe CPU-Auslastung verursachen,
- der Domino-Server auf einer iSeries läuft, auf der weitere interaktive Jobs laufen.

Um geschwindigkeitsbeeinflussende Parameter gezielt einstellen und somit Laufzeit- bzw. Performance-Problemen vorbeugen zu können, wird zunächst eine eigene Klasse für die Domino-Anwendungen erstellt:

```
CRTCLS CLS(QUSRNOTES/DOMPTY30) RUNPTY(30)
```

Die Jobs in dieser Klasse sollen mit der Ausführungspriorität 30 abgearbeitet werden.

Wie alle Objekte im Domino-Umfeld, so muss auch dieses neue Objekt dem Eigner „QNOTES“ zugeordnet werden:

```
CHGOBJOWN OBJ(QUSRNOTES/DOMPTY25) OBJTYPE(*CLS)
NEWOWN(QNOTES)
```

Mit der nachfolgenden Angabe kann festgelegt werden, welche Domino-Tasks in dieser neuen Klasse ausgeführt werden sollen. Existiert in dem unten angegeben Verzeichnis noch keine Datei mit der Bezeichnung „domino_classes“, dann wird diese automatisch mit dem Befehl „EDTF“ erstellt. Anderenfalls kann der bereits vorhandene Inhalt mit diesem Befehl bearbeitet werden:

EDTF ('/qibm/userdata/lotus/notes/domino_classes')

Der Inhalt dieser Datei kann folgendermaßen aussehen:

SERVER=*servername*

CLASS=*classname*

TASKS=*taskname*

Konkret könnte das für den Server „ASDOMZEBIS“ sowie die Tasks „UPDATE“ und „REPLICA“ wie folgt aussehen:

SERVER=ASDOMZEBIS

CLASS=DOMPTY30

TASKS=UPDATE, REPLICA

Diese beiden Tasks würden nach einem Server-Neustart mit der Ausführungspriorität „30“ auf dem System ausgeführt werden.

4.2.5.2 iSeries-Systemwerte

Systemwerte „QDYNPTYADJ“ und „QDYNPTYSCD“

Die beiden Systemwerte „QDYNPTYADJ“ und „QDYNPTYSCD“ werden in Verbindung miteinander eingesetzt.

Der Systemwert QDYNPTYADJ („Dynamische Anpassung der Priorität“) wirkt sich insbesondere bei iSeries-Modellen aus, die sowohl eine interaktive als auch eine Batch-Verarbeitung unterstützen. Dieser Systemwert beeinflusst die interaktive Leistung der Maschine zugunsten der Ausführung von Batch-Jobs. Der Systemwert hat nur dann eine Bedeutung, wenn QDNYPTYSCD („Dynamischer Prioritäts-Scheduler) aktiviert ist. Als Standardwert wird QDNYPTYADJ mit der Einstellung „1“ (= aktiviert) ausgeliefert. Soll der Systemwert geändert werden, wird die Änderung erst nach einem IPL wirksam!

Der zweite in diesem Zusammenhang wichtige Systemwert ist QDYNPTYSCD. Er steuert die Aktivierung bzw. Deaktivierung des dynamischen Prioritäts-Planers. Dieser Systemwert hat als Default-Einstellung den Wert „1“ (=aktiviert). Eine Änderung wird erst nach einem IPL wirksam.

Wenn Domino auf der iSeries installiert und ausgeführt wird, dann sollten diese beiden Systemwerte auf jeden Fall aktiviert sein!

Systemwert „QPRCMLTTSK“ (Prozessor-Multitasking)

Mit dem Erscheinen der OS/400-Release-Version V5R2M0 wurde der Systemwert QPRCMLTTSK eingeführt. Damit wird die Akti-

vierung der Prozessor Multi-Tasking Capability aktiviert. Dieser Systemwert hat zur Folge, dass ein einzelner iSeries-Prozessor sich wie zwei separate Prozessoren verhält. Diese Möglichkeit bieten allerdings nur neuere iSeries-Prozessoren (ab den Modell-Reihen 8xx). Wird OS/400 V5R2M0 auf einem älteren iSeries-Modell installiert, dann wird der Systemwert, der per Standard auf „1“ (Aktiv) steht, beim nächsten IPL automatisch auf „0“ (=deaktiviert) gestellt.

Änderungen an diesem Systemwert wirken sich erst nach dem nächsten IPL aus.

Systemwert „QACTJOB“ (anfängliche Anzahl aktiver Jobs)

Der Systemwert QACTJOB kontrolliert die maximale Anzahl aktiver Jobs im System. Dieser Wert ist in der Standardauslieferung auf „20“ voreingestellt – für eine Domino-Installation auf iSeries sicher zu gering (im Übrigen ist dieser Wert auch bei den meisten anderen iSeries-Installationen, die kein Domino auf der iSeries haben, zu gering eingestellt). Die optimale Einstellung dieses Systemwerts erfolgt am besten nach der folgenden Methode:

Mit dem Befehl WRKACTJOB wird die Auflistung aller aktiven Jobs im System angezeigt. Im oberen rechten Bereich der Anzeige befindet sich die Gesamtanzahl der aktiven Jobs im System. Notieren Sie sich diese Anzahl. Dies sollte zu mehreren Zeitpunkten mit hoher Systemauslastung erfolgen. Anschließend wird auf die Durchschnittssumme der Werte 10 Prozent aufgeschlagen und das Ergebnis wird im Systemwert QACTJOB festgelegt.

Änderungen an diesem Systemwert wirken sich erst nach dem nächsten IPL aus.

Systemwert „QADLACTJ“ (zusätzliche Anzahl aktiver Jobs)

Der Systemwert QADLACTJ gibt die maximale Anzahl zusätzlicher Jobs an, sobald die maximale Anzahl der aktiven Jobs (aus dem Systemwert QACTJOB) erreicht ist. Für jeden weiteren Job werden im System mindestens 110 KB Hauptspeicher reserviert.

Der Wert ist in Abhängigkeit vom Hauptspeicher einzustellen.

4.2.5.3 Datenzugriff

4.2.5.3.1 IFS Type1 / IFS Type2

Die Domino-Integration auf der iSeries ist zu einem großen Teil über das integrierte File System (IFS) der iSeries realisiert. Das IFS existiert bereits seit mehreren Jahren in Form des so genannten „Type1“.

Seit der OS/400-Version V4Rx wurde ein neuer IFS-Typ eingeführt, der wesentliche Änderungen im Aufbau und in der Verarbeitung aufweist. Dieser neue Typ – als „Type2“ bezeichnet – zeichnet sich unter anderem durch eine verbesserte Performance aus. Und diese macht sich gerade im Domino-Umfeld positiv bemerkbar.

Neue iSeries-Modelle werden mit dem IFS – konfiguriert auf Type2 – ausgeliefert. Bei Datenübernahmen wird, so zeigt die Praxis, oft versäumt, die Umstellung des IFS von Type1 auf Type2 durchzuführen, so dass heute eine Vielzahl der Installationen mit dem „alten“ IFS-Type1 betrieben werden. Dabei ist eine Umstellung –

zumindest seit dem OS/400-Release V5R2M0 – recht einfach: durch die Angabe des Befehls CVTDIR.

Sind Sie sich nicht sicher, welcher IFS-Typ auf Ihrem System oder besser für ihre Domino-Files verwendet wird, dann kann dies folgendermaßen festgestellt werden.

In einer OS/400-Befehleszeile wird folgender Befehl angegeben:

DSPLNK OBJ(‚/NOTES/DATA/admin4*‘) OUTPUT(*PRINT) OBJTYPE(*STMF) DETAIL(*EXTENDED) DSPOPT(*ALL)

Ist das dem Domino-Server zugeordnete Verzeichnis nicht bekannt, dann kann dieses mit dem Befehl WRKDOMSVR sowie mit zweimaligem Drücken der F11-Taste angezeigt werden.

```
                          Work with Domino Servers
                                                                 System:   ASZEBIS
Type options, press Enter.
  1=Start server     2=Change server   5=Display console   6=End server
  7=Submit command   8=Work console    9=Work server jobs
  11=Change current directory   12=Work object links   13=Edit NOTES.INI

     Domino
Opt  Server                 Subsystem   Path
     ZEBDOM01           |   DOMIN000    /notes/data
     QPDOMSVR               QPDOMSVR    /Domino/QPDOMSVR









                                                                        Bottom
Parameters or command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F10=Sort by name
F11=Display status    F12=Cancel   F17=Top       F18=Bottom   F24=More keys
```

WRKDOMSVR

Durch den Befehl DSPLNK wird eine Spool-Ausgabe erzeugt, in der sich unter anderem die Angabe über das verwendete File-Format – also über den IFS-Typ – befindet. Finden Sie dort die Angabe „Type2“, dann wird der Domino-Server auf der iSeries bereits mit dem Typ, der von beiden optimaler ist, betrieben. Anderenfalls empfiehlt sich die Konvertierung auf den IFS-Type2 mit der Verwendung des Befehls CVTDIR.

```
                              Spool-Datei anzeigen
Datei . . . . . :   QSYSPRT                          Seite/Zeile 1/1
Steuerung . . . .                                    Spalten     1 - 78
Suchen  . . . . .   Dateiformat
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+...
                 Objektverbindungen anzeigen                        Seite     1
5722SS1 V5R2M0  020719                          ASZEBIS  23.03.04  11:41:35
 Objekt . . . . . :   /notes/data/admin4*
 Objektart  . . . . . :   *STMF
 Detail . . . . . :   *EXTENDED
 Anzeigefunktion  . . :   *ALL
 Verzeichnis  . . . :   /notes/data
 Objektverbindung        Art              Attribut      Text
 admin4.nsf              STMF
 admin4.ntf              STMF
                    Attribute anzeigen                              Seite     2
5722SS1 V5R2M0  020719                          ASZEBIS  23.03.04  11:41:35
 Objekt . . . . . :   /notes/data/admin4.nsf
 Art  . . . . . :   STMF
 Datei-ID . . . . . :   X'00000000000000000186ECB6D30000A1A3
 Eigner . . . . . :   QNOTES
 Zu archivieren (PC)  . . . . . :   Ja
 Zu archivieren (AS/400)  . . . . . :   Ja
 Datum/Uhrzeit des letzten Zugriffs . . :   07.03.04  21:53:20
 Datum/Uhrzeit der Datenänderung  . . . :   07.03.04  21:38:20
 Datum/Uhrzeit der Attributänderung . . :   07.03.04  21:38:20
 Objektgröße in Byte  . . . . . :   2128896
 Zugeordnete Objektgröße  . . . . . :   2359296
 Dateiformat  . . . . . :   *TYPE2
 Größe der erweiterten Attribute  . . . :   0
 Freigegebener Speicher . . . . . :   Nein
 Plattenspeicheroption  . . . . . :   *NORMAL
                                                                  Weitere ...
F3=Verlassen  F12=Abbrechen   F19=Links   F20=Rechts   F24=Weitere Tasten
```

Spool-Anzeige

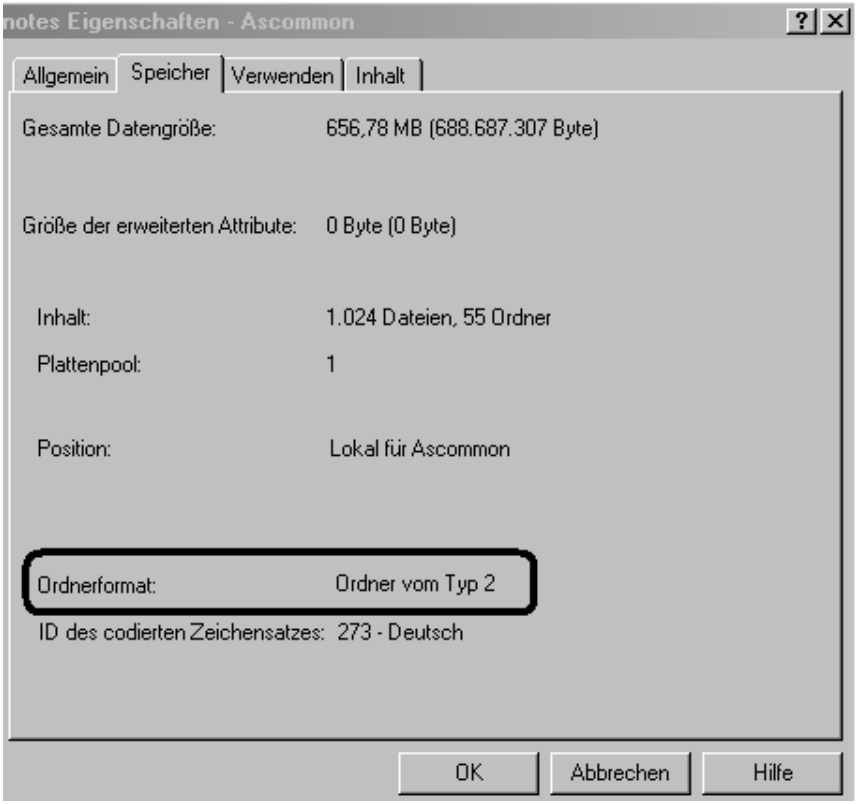
Wem dieses Verfahren zu umständlich ist, der sollte wie folgt vorgehen:

Der IFS-Typ kann auch in dem Befehl WRKLNK angezeigt werden. Wenn das Domino-Verzeichnis ausgewählt wurde, dann kann unter Option „8“ der IFS-Typ angezeigt werden.

Selbstverständlich kann der Typ auch unter dem iSeries Navigator anzeigt werden. Dazu wird folgendermaßen verfahren:

- Auswahl des Eintrags „Datei-System/Integriertes Dateisystem“
- Blättern bis zum Domino-Verzeichnis
- Auswahl einer Domino-Datei mit der rechten Maustaste
- Auswahl der Eigenschaften der Domino-Datei

In der Schaltfläche „Storage“ (oder „Speicher“) befindet sich der Eintrag „File Format“ – dies ist der IFS-Typ.



Type in Navigator

Sollte eine Umstellung auf den IFS-Type2 notwendig sein, dann ist zu beachten, dass das Benutzerprofil, mit dem die Konvertierung durchgeführt wird, die Berechtigung *ALLOBJ haben muss. Wenn Verzeichnisse oder Dateien im Verzeichnis „root“ umgesetzt werden müssen, muss sich die iSeries in einem eingeschränkten Mode (ENDSBS *ALL) befinden, damit die IFS-Umsetzung erfolgen kann.

↳ TIPP:

Die Umstellung des IFS-Type1 auf Type2 kann – einmal gestartet – nicht mehr rückgängig gemacht werden. Im Falle eines Job-Abbruchs wird die Umsetzung im Zuge des nächsten IPL der iSeries automatisch durchgeführt. Entsprechend mehr Zeit kann dieser IPL dann in Anspruch nehmen!

Der Benutzer, der die Umsetzung startet, sollte in jedem Fall in seinem Benutzerprofil den Parameter „Maximal erlaubter Speicher“ auf „*NOMAX“ eingestellt haben, damit der Job fehlerfrei durchläuft.

```
                    Benutzerprofil anzeigen - Basis

Benutzerprofil . . . . . . . . . . . . . . :   ZEIG

Einheitensitzungen begrenzen . . . . . . . :   *SYSVAL
Tastaturpufferung  . . . . . . . . . . . . :   *SYSVAL
Speicherinformationen:
  Maximal erlaubter Speicherplatz  . . . . :   *NOMAX
  Belegter Speicherplatz . . . . . . . . . :   4092520
  In unabh. ASP verwendeter Speicher . . . :   *NO
Höchste Planungspriorität  . . . . . . . . :   0
Jobbeschreibung  . . . . . . . . . . . . . :   ZEIG
  Bibliothek . . . . . . . . . . . . . . . :     QGPL
Berechnungscode  . . . . . . . . . . . . . :
Nachrichtenwarteschlange . . . . . . . . . :   ZEIG
  Bibliothek . . . . . . . . . . . . . . . :     QUSRSYS
Zustellung der Nachrichten aus der
  Warteschlange  . . . . . . . . . . . . . :   *NOTIFY
Bewertung der Nachrichtenwarteschlange . . :   00
                                                                Weitere ...
Eingabetaste --> Weiter

F3=Verlassen   F12=Abbrechen
```

DSPUSRPRF

Für alle iSeries-Betreiber, die das OS/400-Release V5R1M0 einsetzen gilt: Der Befehl CVTDIR ist erst ab V5R2M0 verfügbar. Unter dem Release V5R1M0 kann auch eine IFS-Umstellung mit API „QP0FCVT2“ durchgeführt werden, welche als PTF verfügbar ist.

4.2.5.3.2 Datenbeschaffung

Die Datenbeschaffung der im IFS befindlichen Domino-Daten erfolgt auf der iSeries nach einem bestimmten Verfahren, das sich wesentlich von dem anderer Server-Plattformen unterscheidet.

Domino-Daten befinden sich im internen Datei-System der iSeries und werden auf Anforderung durch die Domino-Anwendung zur Verfügung gestellt. Dabei erfolgt die Übertragung der Daten in Daten-Blöcken (Block Transfer Size).

Im Zuge der Verarbeitung eines Jobs auf der iSeries kann es vorkommen, dass sich die erforderlichen Daten nicht im Hauptspeicher des Systems befinden. Ein solcher Fall wird als Seiten-Fehler (Page Error) bezeichnet.

Block Transfer Size legt fest, wie viel Bytes im Falle eines Page Errors in den Speicher geschrieben werden.

Diese Page Errors haben einen wesentlichen Einfluss auf die Performance – und das nicht nur bei Domino-Anwendungen! Als Regel gilt: Die fehlerhaften Seiten sollten ein 1/10 der gelesenen Seiten nicht übersteigen.

```
            Mit Systemstatus arbeiten                    ASZEBIS
                                                           23.03.04  14:28:07
% CPU benutzt  . . . . . :        0,4    Zusatzspeicher:
% DB-Kapazität . . . . . :        0,0      System-ASP . . . . . :    175,8 G
Abgelaufene Zeit . . . . :   00:00:04      % System-ASP benutzt . :    27,7868
Jobs im System . . . . . :       2838      Gesamtsumme  . . . . . :    175,8 G
% perm. Adressen . . . . :      0,007      Unges. Platz akt.
% temp. Adressen . . . . :      0,010        belegt . . . . . . . :     2677 M
                                          Max. ungeschützt . . . :     2792 M
Änderungen (falls zulässig) eingeben und die Eingabetaste drücken.


System    Pool-    Reserv.    Max.  -DB-Seiten--  --Nicht-DB--
 Pool   Größe(M)  Größe (M)  Aktiv  fehl.  geles  fehl.  geles
   1      219,30     120,32  +++++    0,0    0,0    0,4    2,1
   2     3296,56       1,05     94    0,0    0,0    0,0    0,0
   3      505,29       0,01    185    0,0    0,0    1,1    1,6
   4        0,25       0,00      1    0,0    0,0    0,0    0,0
                                                                  Ende
Befehl
===>
F3=Verlassen          F4=Bedienerführung   F5=Aktualisieren   F9=Auffinden
F10=Erneut starten    F11=Übergangsdaten   F12=Abbrechen   F24=Weitere Tasten
```

WRKSYSSTS

Mit dem Erscheinen des OS/400-Release V5R2M0 wurde eine neue Möglichkeit geschaffen, Page Errors zu beeinflussen. Der Befehl CHGATR – bereits seit einigen OS/400-Release-Versionen verfügbar – wurde um die Eingabemöglichkeit „*MAINSTGOPT“ erweitert. Damit können die Hauptspeicherzuordnungen angepasst werden. Dieser Wert kann mit drei unterschiedlichen Einstellungen versehen werden:

- ***normal**
  - zu verwenden bei „ausreichendem“ Hauptspeicher
  - Block Size-Größe: 16KB
  - Reduzierung der Plattenzugriffe durch Übertragung größerer Blöcke

- ***minimize**
  - zu verwenden bei „knappem“ Hauptspeicher
  - Block Size-Größe: 8KB
  - „aggressive“ Hauptspeicherverwaltung durch „Platzschaffung“ in Form von Auslagerung anderer Hauptspeicherbereiche
- ***dynamic**
  - zu verwenden in Kombination mit Pool-Einstellung *CALC
  - Block Size-Größe: 12KB

Je nach Hauptspeicherausstattung der iSeries kann die Verwendung der drei Einstellungsmöglichkeiten mehr oder weniger sinnvoll sein. Die Einstellung „*dynamic“ hat sich in der Praxis durchaus bewährt.

Soll die Einstellung geändert werden, kann der Domino-Server aktiv bleiben. Die Einstellungen können global für alle Domino-Dateien vorgenommen oder selektiv auf einzelne Dateien angewendet werden:

Der Befehl

CHGATR OBJ(‚/NOTES/DATA/MAIL/wwinzig.nsf‘) ATR(*MAINSTGOPT) VALUE(*DYNAMIC)

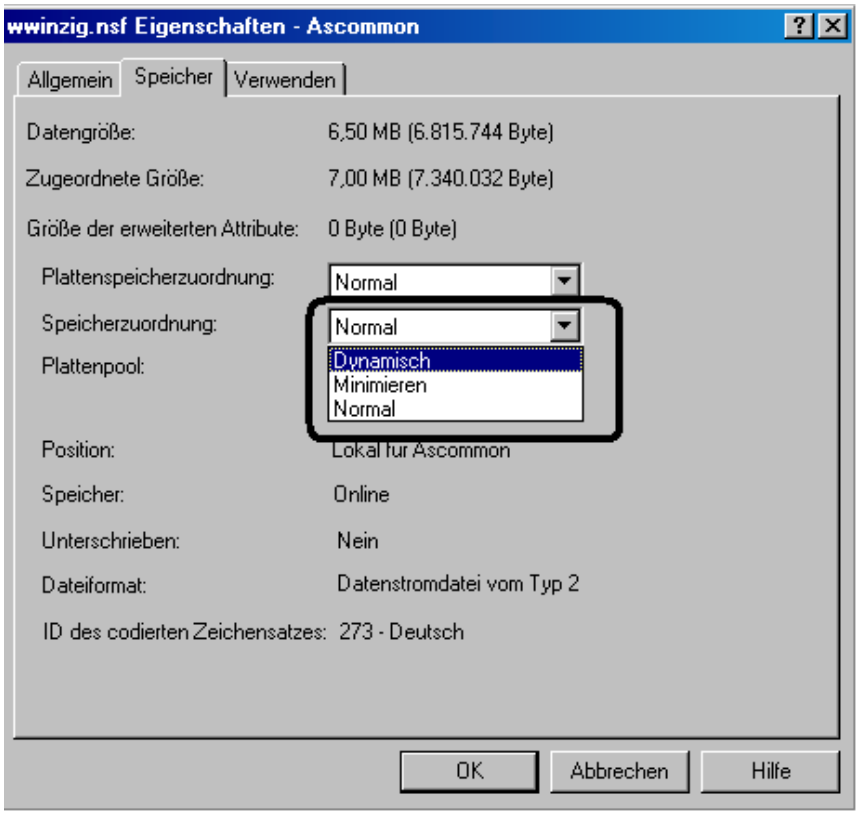
ändert eine einzelne Mail-Datenbank.

Der Befehl

CHGATR OBJ(‚/NOTES/DATA/MAIL/*‘) ATR(*MAINSTGOPT) VALUE(*DYNAMIC)

ändert alle Mail-Datenbanken.

Selbstverständlich können die Einstellungen auch mit dem iSeries Navigator vorgenommen werden. Dazu wird die Datei mit der rechten Maustaste markiert und in den Eigenschaften des Speicherbereichs ausgewählt. Die Block Size kann dann geändert werden.



Speicherzuordnung

4.2.5.3.3 Authority Lookups

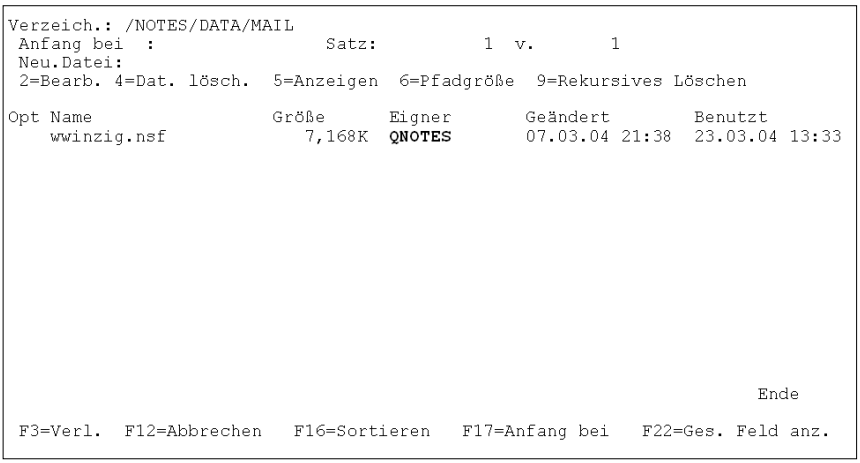
IBM bietet mit dem Lizenzprogramm „Performance Tools“ ein elegantes Werkzeug, um die Leistungsdaten der iSeries auszuwerten und um dann diese Auswertungen für die Optimierung des Systems zu verwenden. Wer dieses Tool bereits nutzt, wird vielleicht festgestellt haben, dass eine Vielzahl der Einträge, die während der Laufzeit des Tools gesammelt werden, durch so genannte „Authority Lookup Exceptions“ verursacht werden.

Diese Authority Lookups zeigen an, ob ein Benutzer berechtigt ist, ein OS/400-Objekt zu verwenden. Ist er es nicht, dann wird ein entsprechender Protokolleintrag erzeugt, der auf diesen unerlaubten Zugriff hinweist. Leider erfordert dieser Protokolleintrag jeweils CPU-Arbeitszeit – und das kann sich bei Häufung von Nicht-Berechtigungen tatsächlich spürbar auswirken. Diese Eintragungen können mittels des Performance-Tools ermittelt werden.

Zwar haben sich diese Performance-Auswirkungen mit den schnelleren und größeren Systemen reduziert. Allerdings kann auch bei diesen Maschinen in Grenzbereichen, in denen mehrere Performance-Faktoren das System negativ beeinflussen, die korrekte Berechtigungsvergabe wesentlich für die allgemeine Leistung sein.

Die allgemeinen Domino-Objekte haben den Eigner „QNOTES“. Für den allgemeinen Zugriff sollten diese Objekte den Zugriff über „*public“ ermöglichen.

Ist nicht sicher, wer der Eigner der Domino-Objekte ist, dann kann mit dem nachfolgenden Verfahren festgestellt werden, welche Objekte welchem Eigner zugeordnet sind.



Verzeichnis anzeigen

Ist der Eigner nicht das Benutzerprofil „QNOTES“, dann sollte er geändert werden. Achten Sie unbedingt darauf, dass es sich um Standard Notes-Objekte handelt. Einige auf Domino basierende Anwendungssysteme verwenden als Eigner andere Benutzer!

4.2.5.3.4 Transaction Logging

Mit der Domino-Version 5 wurde das so genannte „Transaction Logging" eingeführt. Ursprünglich für Performance-Optimierungen ausgelegt, dient das Transaction Logging auf der iSeries u. a. als eine Basisvoraussetzung für die inkrementellen Datensicherungen von Domino auf der iSeries unter Verwendung von BRMS.

Leider kann der ursprüngliche Ansatz des Transaction Logging – nämlich die Performance-Optimierung – genau ins Gegenteil umschlagen, wenn Transaction Logging nicht korrekt installiert wurde. Dann können durchaus massive Performance-Probleme auftreten.

Diese Performance-Probleme können dann auftreten, wenn die Plattenauslastungen – oder besser: die Lastverteilung (im Englischen sprechen wir von Load-Balancing) – nicht optimal ist, denn Transaction Logging erhöht die Last der Schreib- und Lesezugriffe auf die Platten.

Sind Sie nicht sicher, ob der Plattenspeicher Ihrer iSeries die Last optimal verteilt hat, dann kann dies wie folgt ermittelt werden:

- **WRKDSKSTS**
- F5-Taste drücken
  - Damit wird die Anzeige automatisch aktualisiert.
- Überprüfen der Plattenauslastung für ca. 15 Minuten
  - Spalte mit der %-Auslastung
  - Die %-Auslastung sollte bei allen Platten < 30% sein.

```
              Mit Plattenstatus arbeiten                    ASZEBIS
                                                              23.03.04  13:38:34
Abgelaufene Zeit:   00:00:02

Ein-          Größe  %be-    E/A   Anford.  Lese   Schrb.  Lesen  Schrb  %ver-
heit  Typ      (M)   legt   Anf.  Größe(K)  Anf.   Anf.    (K)    (K)   wend.
   1  4326  26373  27,5    0,7      4,0     0,7     0,0    4,0    0,0     0
   2  4326  26373  27,5    0,3      4,0     0,3     0,0    4,0    0,0     0
   3  4326  35165  27,5    0,7      4,0     0,7     0,0    4,0    0,0    20
   4  4326  35165  27,5    0,3      4,0     0,3     0,0    4,0    0,0     0
   5  4326  26373  27,5    1,4      4,0     1,4     0,0    4,0    0,0    20
   6  4326  26373  27,5    1,0      9,3     1,0     0,0    9,3    0,0     0









                                                                        Ende
Befehl
===>
F3=Verlassen   F5=Aktualisieren   F12=Abbrechen   F24=Weitere Tasten
```

DSPDSKSTS

Ist die %-Auslastung aller Platten größer als 30 Prozent, dann hat die iSeries ein Load-Balancing-Problem, dass nicht nur die Domino-Anwendungen negativ beeinflusst, sondern die gesamte Performance der iSeries tangiert. Dieser Hinweis gilt also nicht nur in Verbindung mit Domino, sondern ist ein genereller Richtwert, der auf der iSeries nicht überschritten werden sollte.

Sind mehrere Platten mit einer %-Auslastung von mehr als 30 Prozent ermittelt worden, dann spricht man von dem so genannten „Disk constrained“.

Ist die %-Auslastung größer als 30 Prozent, dann kann das Transaction Logging von Domino der berühmte Tropfen auf dem heißen Stein sein und die Gesamtleistung der iSeries stark negativ beeinflussen. IBM empfiehlt in einem solchen Fall die Reduzierung der

Last der Plattenzugriffe – allerdings wohl eher eine praxisfremde Empfehlung.

Wirklichen Erfolg kann man in einem solchen Fall in der Regel nur durch die Erweiterung des Platten-Pools, sprich durch Hinzufügen weiterer Platten erzielen, die durch zusätzliche Zugriffsarme die Last-Verteilung und die Datenbeschaffung positiv beeinflussen.

Wer diese Möglichkeit hat, sollte erwägen, das Transaction Logging für Domino in einem eigenen Benutzer-ASP einzurichten. Dieses Benutzer-ASP bedingt allerdings eigene Plattenkapazitäten, die diesem ASP exklusiv zur Verfügung stehen. Damit wird die eigentliche Domino-Installation, die sich in einem anderen ASP befinden sollte, nicht negativ beeinflusst.

Mit der Version 6 des Domino-Servers hat IBM das Transaction Logging um das View Logging erweitert. Damit besteht die Möglichkeit, Ansichtsinformationen im Transaction Log zu speichern. Das bringt im Falle einer Wiederherstellung nach einem Systemausfall eine wesentliche Zeitersparnis mit sich – allerdings mit dem Nebeneffekt, dass sich das View Logging negativ auf die Performance des Servers auswirkt.

4.2.5.3.5 Domino-Speichermanagement

Der Domino-Server – und das unabhängig von der iSeries – geht stets davon aus, dass für Domino der gesamte Speicher des Servers exklusiv zur Verfügung steht. In der Praxis dürfte das allerdings nur hin und wieder zutreffen. Im speziellen Fall der iSeries wohl nur dann, wenn Domino auf einem Dedicated Domino-Server installiert ist.

Anderenfalls muss Domino sich die Systemressourcen mit anderen Anwendungen teilen – und das auch dann, wenn mehrere Domino-Server in Partitionen installiert sind. Dann müssen sich diese partitionierten Server ebenfalls den Hauptspeicher teilen, was zur Folge hat, dass die Paging- und Fault-Werte der einzelnen Server stark ansteigen und die Gesamtleistung des Systems negativ beeinflusst wird. Damit dieser Effekt möglichst nicht zu stark auftritt, kann durch geschickte Systemeinstellungen die Gesamtleistung der einzelnen Anwendungen optimal eingestellt werden.

Domino verfügt über ein eigenes Speichermanagement, das auf das iSeries-Speichermanagement aufsetzt.

In diesem Zusammenhang ist es wichtig zu verstehen, wie Domino auf der iSeries in Hinsicht auf die Hauptspeicherzuordnung arbeitet.

Domino auf der iSeries läuft in einem so genannten Speicher-Pool (Storage oder auch Memory Pool). Dies sind Teilbereiche des Hauptspeichers, die nach unterschiedlichen Gruppierungen der Anforderungen der auszuführenden Jobs zusammengefasst sind. Die automatische Leistungsanpassung der iSeries ermöglicht eine Hauptspeicherverteilung zwischen den einzelnen Pools je nach aktueller Systemanforderung.

Dies kann unter Umständen zur Folge haben, dass einige Jobs anderen Bereichen Ressourcen entziehen, wodurch die Bereiche, deren Speicherzuordnung reduziert wurde, langsamer laufen.

Domino läuft in der Standard-Konfiguration in dem *BASE-Pool (das ist der zweite Pool in der WRKSYSSTS-Anzeige).

```
                          Mit Systemstatus arbeiten                    ASZEBIS
                                                              23.03.04  14:28:07
% CPU benutzt  . . . . . :         0,4    Zusatzspeicher:
% DB-Kapazität . . . . . :         0,0      System-ASP . . . . . :     175,8 G
Abgelaufene Zeit . . . . :    00:00:04      % System-ASP benutzt . :    27,7868
Jobs im System . . . . . :        2838      Gesamtsumme  . . . . . :    175,8 G
% perm. Adressen . . . . :       0,007      Unges. Platz akt.
% temp. Adressen . . . . :       0,010        belegt . . . . . . . :     2677 M
                                            Max. ungeschützt . . . :     2792 M
Änderungen (falls zulässig) eingeben und die Eingabetaste drücken.


System    Pool-     Reserv.    Max.
 Pool   Größe(M)  Größe (M)  Aktiv  Pool        Subsystem   Bibliothek
   1      219,30     120,32  +++++  *MACHINE
   2     3296,56       1,05     94  *BASE
   3      505,29       0,01    185  *INTERACT
   4        0,25       0,00      1  *SPOOL
                                                                    Ende
Befehl
===>
F3=Verlassen          F4=Bedienerführung   F5=Aktualisieren   F9=Auffinden
F10=Erneut starten    F12=Abbrechen        F24=Weitere Tasten
```

WRKSYSSTS

Oder es läuft im iSeries Navigator:

Pool	Beschreibung	Aktuelle Größe	Aktuelle	Maximal auswählbare	Summe der
Maschine	Von internen Maschinenfunktione...	217,61	48	Kein Maximum	0,0
Basis	Standard-Systempool	2.814...	380	94	0,9
Interaktiv	Für interaktive Arbeit benutzt	989,09	5	185	0,0
Spool	Zum Drucken benutzt	0,25	0	1	0,0

Pools

Hier gibt es im Hinblick auf die Leistungsoptimierung von Domino zwei Speicher-Pools, die betrachtet werden müssen:

Der Maschinen-Pool (*Machine)

Der Maschinen-Pool ist immer der erste Pool in der Anzeige des Systemstatus WRKSYSSTS. Der Maschinen-Pool übernimmt die Kommunikation des Licensed Internal Code (LIC) und der Kommunikationsdaten (z.B. TCP/IP).

Die Größe des Maschinen-Pools wird in dem Systemwert QMCHPOOL angegeben. Änderungen an diesem Systemwert sollten mit Bedacht durchgeführt werden – denn wenn dieser Wert zu klein gewählt wird, dann kann die gesamte Leistung der iSeries ausgebremst werden! Der Auslieferungswert ist mit 20.000 KB voreingestellt, er kann aber durch einen aktiven QPFRADJ jederzeit eingepasst werden. Sobald QPFRADJ läuft, braucht sich der Administrator keine Gedanken mehr um den QMCHPOOL zu machen.

Ist der Einsatz von QPFRADJ nicht gewünscht oder nicht möglich (z.B. im SAP-Umfeld), dann kann die optimale Größe des QMCHPOOL nach einem einfachen Verfahren ermittelt und dann manuell eingestellt werden:

- Ausführen des Domino-Servers über mehrere Tage
- zu hohen Auslastungszeiten den Wert „Reserved Size“ für den *MACHINE Pool in dem Befehl WRKSYSSTS ermitteln
- Einstellen des doppelten Wertes von „Reserved Size“ in QMCHPOOL

z.B.:

1. WRKSYSSTS
2. Reserved Size ermitteln
3. CHGSYSAL SYSVAL(QMCHPOOL)
   VALUE(xxxxxxxxxxxxxxxxxxxx)

↳ **Achtung!**
Wird der Systemwert QMCHPOOL mit dem Green-Screen-Befehl CHGSYSVAL geändert, dann muss der Wert in KB angegeben werden. Wird die Änderung mit dem iSeries Navigator durchgeführt, dann muss diese dort in MB vorgenommen werden!

4.2.5.4 Domino Performance-Einstellungen

Zuvor wurden die Performance-Aspekte auf der iSeries betrachtet. Es gibt auch einige Einstellungsmöglichkeiten auf Seiten des Domino-Servers, die sich wesentlich auf die Geschwindigkeit auswirken können.

Einige dieser Möglichkeiten werden nun im Weiteren behandelt.

Update Task:
Ein häufiger Grund für schlechte Performance von Domino auf der iSeries liegt darin, dass der Update Task unnötige Aktionen durchführt. Der Update Task ist für das Aktualisieren und die Wiederherstellung von Indizes von Domino-Ansichten verantwortlich. Damit soll vermieden werden, dass ein Benutzer beim Aufruf einer Ansicht längere Wartezeiten für die Indexierung in Kauf nehmen muss.

Sobald eine Änderung in einer Domino-Datenbank durchgeführt wurde, wird ein entsprechender Eintrag geschrieben, der den Update Task dieser Datenbank verarbeiten lässt.

Der Update Task wird in der Regel automatisch ausgeführt, kann aber auch manuell aufgerufen werden.

Die Einstellung, ob der Task automatisch ausgeführt werden soll, befindet sich in NOTES.INI – in dem Eintrag der Server Tasks:

ServerTasks=Replica,Router,**Update**,Stats,AMgr,AdminP,Sched,...

Updall Task:
Eine Komponente des Update Task ist der Updall Task. Dieser Task wird meist einmal täglich ausgeführt. Er aktualisiert die Ansichten aller Notes-Datenbanken. Wann dieser Task ausgeführt werden soll, kann ebenfalls in NOTES.INI eingestellt werden. Per Default wird dieser Task um 02.00 ausgeführt:

ServerTasksAt2=**Updall**

Für die Verarbeitungsgeschwindigkeit einer Datenbank in einem Update Task ist die Anzahl der Dokumente maßgebend.

Wesentliche Performance-Einbußen können durch den Update Task bei den folgenden Konstellationen auftreten:

- Die Gesamtanzahl der Dokumente innerhalb der Ansichten der Notes-Datenbank ist extrem hoch.
- Die Erstellung eines Vollindexes ist für die Datenbank angegeben.

- Viele Ansichten (in großen Datenbanken) müssen komplett wiederhergestellt werden.
- Viele Ansichten enthalten zeitabhängige Selection Formulas (automatischer Update der Ansicht).

Um eine Analyse des UPDATE Task durchzuführen, geht man am besten wie folgt vor:

❶❷❸ Ausführungsschritte:

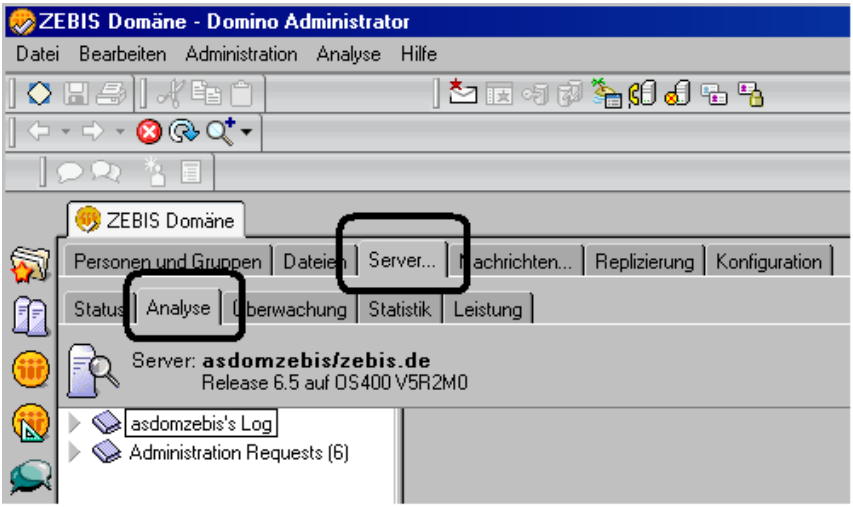
1. Hinzufügen des Eintrages LOG_UPDATE=2 in NOTES.INI
   Damit werden Ansichtsaktualisierungen protokolliert.

2. Stoppen und Starten des UPDATE Tasks
   – Tell UPDATE quit
   – Load UPDATE

3. Sammeln von Daten während Zeiten hoher CPU-Auslastung

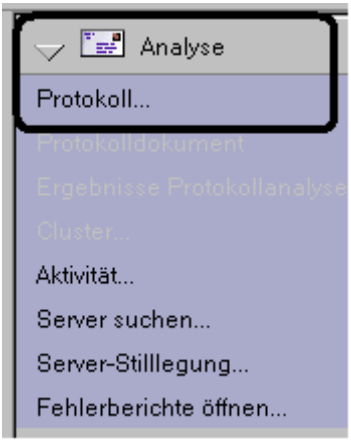
4. Beenden der Protokollierung
   Entfernen des NOTES.INI-Eintrages.

5. Filter auf die Log-Datei setzen



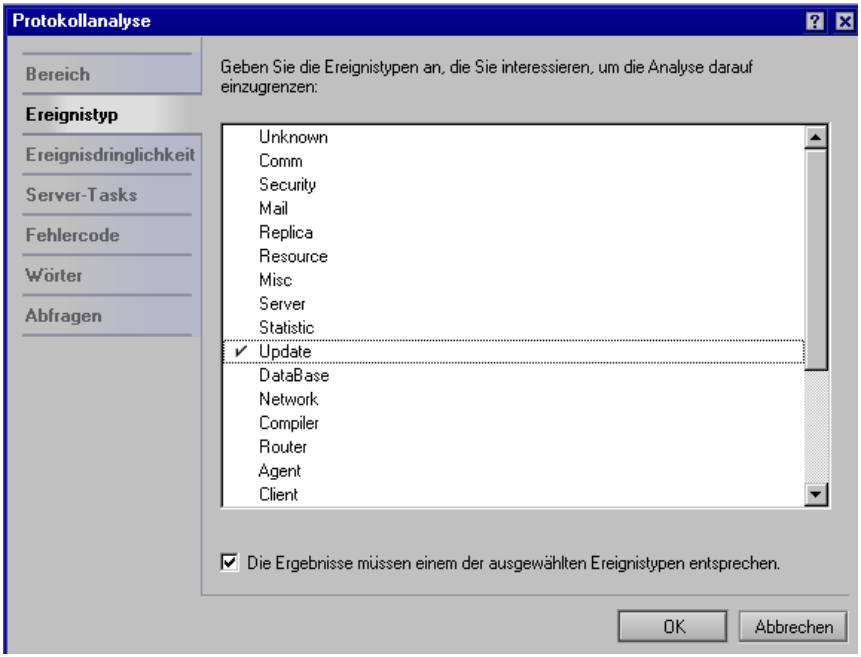
Protokoll-Filter

Im rechten Bereich der Maske kann das Protokoll bearbeitet werden:



Protokoll-Filter angeben

Es können unterschiedliche Filter für das Protokoll angegeben werden.



Update-Selektion

NSF_BUFFER_POOL_SIZE_MB

Domino arbeitet in vielen Bereichen mit so genannten Buffer Pools. Das sind Bereiche, in denen Informationen zwischengespeichert werden und nicht erst auf Anforderung von der Platte gelesen werden müssen. Einige dieser Pools sind fix eingestellt und lassen sich nicht administrieren, andere dagegen können individuell angepasst werden. Allerdings können Anpassungen neben den gewünschten Effekten natürlich auch unerwünschte Ergebnisse zur Folge haben – in diesem Fall eben schlechte Performance-Daten.

Nachfolgend werden einige dieser Buffer Pools näher betrachtet, die in Domino angepasst werden können.

Der Parameter NSF_BUFFER_POOL_SIZE_MB befindet sich in NOTES.INI und definiert den I/O-Transfer zwischen Notes Index Facility (NIF) und Plattenspeicher. Ist dieser Parameter nicht in NOTES.INI angegeben, dann wird als Default-Einstellung 3/8 des verfügbaren Speichers des jeweiligen Pools als NSF Buffer Pool verwendet.

Eine kleine Anmerkung zwischendurch:
NIF hat sich in Domino 6 wesentlich geändert. Nachfolgende Übersicht zeigt dies deutlich:

- Domino Release vor 5.0.10
  25 MB
- Domino 5.0.10 und höhere
  50MB
- ab Domino 6
  100 MB

Der NSF Buffer Pool sollte angepasst werden, wenn:

- er versucht mehr Speicher zu reservieren, als in dem zugeordneten Pool verfügbar ist.
  Ist beispielsweise der Wert des Parameters NSF_BUFFER_POOL_SIZE_MB auf 400 MB gesetzt, der zugeordnete Speicher-Pool der iSeries verfügt aber nur über 300 MB, dann wird versucht, die fehlenden 100 MB Speicher zuzuordnen, was eine Erhöhung der Seitenfehler nach sich zieht. Zwar wird die Performance des Domino-Servers nicht in erster Linie schlechter, aber dieses Phänomen wirkt sich stark auf die allgemeine CPU-Belastung der iSeries aus, was in Grenzauslastungsbereichen massiv negativ sein kann.

  Deshalb gilt hier die Empfehlung:
  NSF_BUFFER_POOL_SIZE_MB sollte nicht größer gesetzt werden als 3/8 des Speichers des Pools, in dem Domino ausgeführt wird.

- Der NSF Buffer Pool ist für den Domino-Server zu klein.
  Die Ausführungsgeschwindigkeit des Domino-Servers verbessert sich stark, wenn Indexinformationen direkt aus dem NSF Buffer und nicht erst von den Platten gelesen werden. Wenn der NSF Buffer zu klein gewählt wurde, dann können die erforderlichen Informationen nicht gespeichert werden und müssen immer auf Anforderung von der Platte der iSeries gelesen werden, was die Geschwindigkeit stark verlangsamt, denn neben den I/O-Operationen wird auch die CPU belastet.

Doch wie sollte nun der Wert des Parameters NSF_BUFFER_POOL_SIZE_MB korrekt gesetzt werden?

Dazu sehen wir uns zunächst mit dem Befehl SHOW STAT DATABASE die aktuellen Einstellungen an. Es ist sinnvoll, dieses Verfahren dann anzuwenden, wenn eine „normale" Auslastung des Domino-Servers durch die Benutzer gegeben ist!

- WRKDOMSVR SERVER(Servername)
- SHOW STAT DATABASE
- F5-Taste drücken
- F6-Taste drücken, um einen Ausdruck zu erzeugen

Dieses Verfahren soll ca. vier bis fünfmal innerhalb einer Stunde wiederholt werden. Durch das Drücken der F6-Taste wird jeweils eine Spool-Datei QSYSPRT erstellt. Die wichtigen Parameter in diesem Zusammenhang sind:

- **Database.Database.BufferPool.Maximum.Megabytes**
  Dieser Wert sollte mit dem Wert von NSF_BUFFER_POOL_SIZE_MB übereinstimmen.

- **Database.Database.BufferPool.Peak.Megabytes**
  Dieser Wert zeigt den Peak Amount des zugeordneten Speichers des Domino-Servers und wird jedes Mal nach Beenden des Domino-Servers neu gesetzt.

- **Database.Database.BufferPool.PerCentReadsInBuffer**
  Prozentuale Angabe der gelesenen Informationen aus dem NSF Buffer.

- **Database.DbCache.CurrentEntries**
  Aktuelle Anzahl der Einträge im Datenbank-Cache.

- **Database.DbCache.HighWaterMark**
  Absolute Anzahl von Einträgen im Datenbank-Cache seit dem letzten Serverstart.

- **Database.DbCache.MaxEntries**
  Anzahl der Einträge, die im Datenbank-Cache zwischengespeichert werden können.

```
                              Spool-Datei anzeigen
Datei . . . . . :   QSYSPRT                          Seite/Zeile 1/57
Steuerung . . . .                                    Spalten     1 - 78
Suchen  . . . . .
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+...
03/23/2004 14:35:12   LDAP Server: No ports enabled, listener not started but
 control task running to maintain schema
03/23/2004 14:35:12   LDAP Server: Started
03/23/2004 14:35:13   HTTP Server: Shutdown
03/23/2004 14:35:13   Collection Services Started
> show stat database
  Database.DAFailoverCount = 0
  Database.DARefreshServerInfoCount = 0
  Database.DAReloadCount = 0
  Database.Database.BufferPool.Maximum.Megabytes = 300
  Database.Database.BufferPool.MM.Reads = 0
  Database.Database.BufferPool.MM.Writes = 0
  Database.Database.BufferPool.Peak.Megabytes = 7
  Database.Database.BufferPool.PerCentReadsInBuffer = 98.54
  Database.DbCache.CurrentEntries = 5
  Database.DbCache.HighWaterMark = 5
                                                                  Weitere ...
F3=Verlassen  F12=Abbrechen   F19=Links   F20=Rechts   F24=Weitere Tasten
```

Spool-Datei anzeigen

Der Wert des NSF_BUFFER_POOL_SIZE_MB ist zu klein, wenn folgende Bedingungen zutreffen:

Database.Database.BufferPool.Peak.Megabytes =
Database.Database.BufferPool.Maximum.Megabytes

und

Database.DbCache.HighWaterMark =
Database.DbCache.MaxEntries

oder:

Database.Database.BufferPool.PerCentReadsInBuffer < 95%

und

Database.DbCache.HighWaterMark =
Database.DbCache.MaxEntries

Trifft eine dieser beiden Bedingungen zu, dann sollte der Wert des Parameters entsprechend geändert werden. Anpassungen sollten den bisherigen Wert um maximal 10 Prozent verändern. Anschließend (nach einer gewissen Laufzeit!) sollten die Einstellungen nochmals überprüft werden. Die Änderungen dieses Parameters wirken sich erst nach einem Neustart des Domino-Servers aus!

Der Wert des NSF_BUFFER_POOL_SIZE_MB ist zu groß, wenn:

Database.Database.BufferPool.PerCentReadsInBuffer
zwischen 94% und 99% liegt

aber

Database.DbCache.MaxEntries
ist ca. 40% größer als
Database.DbCache.HighWaterMark

Wenn diese Bedingungen zutreffen, dann kann der Wert des Parameters verkleinert werden. Anpassungen sollten – wie auch bei der Erhöhung des Parameters – ca. 10 Prozent betragen. Die Änderungen werden erst nach einem Neustart des Domino-Servers wirksam.

Der Wert des NSF_BUFFER_POOL_SIZE_MB ist zu optimal, wenn mindestens eine der beiden Bedingungen zutrifft:

1. *Database.DbCache.MaxEntries* >*Database.DbCache.HighWaterMark* (allerdings sollte die Differenz nicht mehr als 20% betragen)

oder:

2. *Database.Database.BufferPool.PerCentReadsInBuffer* zwischen 94% und 99% liegt (allerdings nur, wenn *Database.DbCache.MaxEntries* ca. gleich ist mit *Database.DbCache.HighWaterMark*).

PercentAvailSysRessources

Dieser Parameter befindet sich ebenfalls in NOTES.INI und ermöglicht die globale Kontrolle aller Buffer Pools. Dabei werden Einstellungen der einzelnen Buffer Pools von diesem Parameter nicht überschrieben.

Z.B. wird der Wert des Parameters NSF_BUFFER_POOL_SIZE_MB nicht von dem Parameter *PercentAvailSysResources* überschrieben, wenn dieser ebenfalls in NOTES.INI angegeben ist.

Wie weiter oben in dieser Session erwähnt, wird jeder Domino-Server sich so verhalten, als würde der gesamte Systemspeicher exklusiv für ihn zur Verfügung stehen. Damit die Auswirkungen dieser Arbeitsweise nicht zu stark die übrigen Applikationen (oder weitere Domino-Server) belasten, kann durch den Parameter PercentAvailSysResources eingestellt werden, wie viel Prozent des Hauptspeichers für diesen Server verwendet werden können.

Je nachdem, in welchem Pool der Domino-Server ausgeführt wird, kann die Prozentangabe eine unterschiedliche Bedeutung haben:

- **im *BASE Pool**
  Kompletter Hauptspeicher dient als Berechnungsgrundlage.
- **im Shared Pool oder privaten Pool**
  Es wird der diesem Pool zugeordnete Speicher als Berechnungsgrundlage verwendet.

Der Wert des Parameters PercentAvailSysResources kann zwischen 2 und 100 Prozent angegeben werden.

Notes_SHARED_DPOOLSIZE

Dieser Parameter befindet sich ebenfalls in NOTES.INI und ist verantwortlich für die globale Steuerung der Datenbank-Buffer (DPOOLS). Damit soll vermieden werden, dass die I/O-Zugriffe auf die Platten uneffektiv sind.

In Domino 5 war die Standard-Größe für diesen Parameter 256 MB; sie wurde in Domino 6 auf 512 MB erweitert.

Je nach Systemanforderungen werden mehrere DPOOLS parallel angelegt, um eine optimale Auslastung zu erreichen. Dies hat allerdings den Nachteil, dass Speicher für diese Pools temporär verloren geht.

Der Parameter kann entweder über NOTES.INI oder über die Umgebungs-Variable gesetzt werden. Letztere setzt den Parameter für alle in dieser Partition installierten Domino-Server.

ADDENVVAR ENVVAR('Notes_SHARED_DPOOLSIZE') VALUE(1048576) LEVEL(*SYS)

Wird der Wert des Parameters zu hoch eingestellt, dann hat das zur Folge, dass eine Vielzahl von DPOOLs erzeugt werden und damit Speicherplatz zeitweise verschwendet wird. Zudem kann die CPU-Auslastung überproportional ansteigen.

Wird der Parameter zu klein gewählt, dann geht dies überwiegend zu Lasten der CPU, wenn nach freiem Speicherplatz in den vorhandenen DPOOLs gesucht wird. Hier haben die neueren POWER4-Prozessoren und deren Nachfolger deutliche Vorteile gegenüber deren Vorgängern, da sie die Verarbeitung der Anforderungen wesentlich besser bewerkstelligen.

Doch wie soll nun dieser Parameter sinnvollerweise eingestellt werden?

Leider gibt es hier keine allgemeingültige Regel für die Einstellung des Parameters, denn er ist in höchstem Maße von individuellen Zusammenspielen einzelner Komponenten abhängig.

Grob gilt in diesem Fall die Checkliste:

- **Wie viele DPOOLs existieren für jeden Domino-Job?**
  - Je geringer die Anzahl der Pools ist, desto weniger Speicher wird benötigt.
    - o Je weniger Pools, desto geringere CPU-Auslastung und geringere Page Faults!
- **Wie viel Prozent werden in den einzelnen DPOOLs belegt?**
- **Wie oft muss der Domino-Server nach freien DPOOLs suchen?**
  - Dies hat einen wesentlichen Einfluss auf die Performance – denn je schneller freier Platz gefunden wird, desto schneller erfolgt natürlich die gesamte Verarbeitung.
- **Wie oft schlägt die Suche nach freiem Platz fehl?**
  - Wenn die Suche nach einem freien Platz in einem DPOOL fehlschlägt, muss erst nach einem anderen DPOOL und in diesem wieder nach freiem Platz gesucht werden.

Diese Informationen können im Speicherprotokoll von Domino gefunden werden.

Dazu wird zunächst der Befehl SHOW MEMORY DUMP an der Domino-Konsole eingegeben. Als Ergebnis wird eine Datei erzeugt, die die gewünschten Informationen enthält.

```
> show memory dump

   > show memory dump

   Memory Available: 2,048 Mbytes

   03/23/2004 14:38:24   Created memory dump file '/notes/data/IBM_TECHNICAL_SUP
   PORT/memory_ASZEBIS_2004_03_23@14_38_20.dmp'
 Enter a Domino subcommand.
 ===>
```

Memory Dump

In diesem Protokoll wird angezeigt, wie viele Pools jeder Domino-Job erzeugt hat. Zudem wird angezeigt, wie viel Speicher von jedem DPOOL belegt wird und wie oft der Domino-Server den DPOOL nach freiem Speicher durchsucht hat.

```
Bearbeit.: /NOTES/DATA/IBM_TECHNICAL_SUPPORT/memory_ASZEBIS
 Satz:       1784   v.    2468 um   8            Spalte:     1    124 um  74
 Strg:

BEF ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+
                          Size   used        free      total   skip     search  failure
    s  3 FB562A4CCA19FF70   512K   256K 50%    223K      324        4      320        3
    s  4 FB562A4CCA21FFC0   512K   256K 50%    256K      244        7      237        1
    s  5 FB562A4CCA29FFD0   512K   257K 50%    256K      162        1      161        1
    s  6 FB562A4CCA320020   512K   256K 50%    256K       65        0       65        1
    s  7 FB562A4CCA3A0030   512K   257K 50%      0b       72        0       72        0
    8 process private memory pools
    3 MB total pools size
    1 MB total pools used

    52.99% pool utilization
    1.03 pools visited per allocation
         0.02 pools skipped
         1.02 pools searched
    1.03 free blocks searched per allocation
    1.06 free blocks searched per free

 F2=Speichern  F3=Speichern/Verl.  F12=Verlassen  F15=Services
 F16=Suche wiederholen  F17=Änderung wiederholen  F19=Links  F20=Rechts
```

Pool-Anzeige

In diesem Beispiel hat der Server-Job sieben DPOOLs und die durchschnittliche Auslastung liegt bei 53 Prozent – das sind sehr gute Werte.

Wenn die Pool-Anzahl größer als 15 ist und die durchschnittliche Auslastung steigt, dann sollte der Wert DPOOL verkleinert werden. Dasselbe gilt auch, wenn die Fehler (failure) 15 Prozent übersteigen.

Wenn die DPOOL-Einstellungen angepasst wurden, dann muss der Domino-Server neu gestartet werden, damit diese Änderungen wirksam werden.

4.3 Installation unter AIX auf IBM RS6000

UNIX war ursprünglich die Server-Plattform für Lotus Notes. Für die verschiedenen UNIX-Derivate von Sun, HP und IBM liegen deshalb schon lange Domino-Versionen vor. Die jüngste UNIX-Version wurde im Jahr 1999 für Linux vorgestellt.

4.3.1 Systemvoraussetzungen

Bevor Lotus Domino auf AIX installiert werden kann, muss überprüft werden, ob Hardware und Betriebssystem für die Einrichtung als Domino-Server geeignet sind. Wie auch bei den anderen Systemen gilt hier, dass ausreichend Ressourcen zur Verfügung stehen müssen und dass jeder weitere Benutzer zusätzliche Ressourcen benötigt.

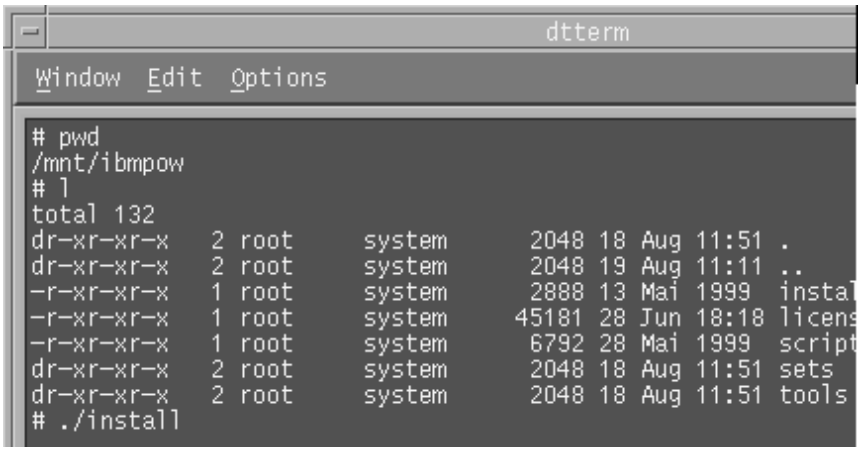
Das Betriebssystem muss IBM AIX 4.3.1 oder höher sein. Der PTF-Stand muss überprüft und gegebenenfalls angepasst werden. Nach dem Einspielen der PTFs kann es erforderlich sein, das System neu zu booten.

Für Domino müssen ein Benutzer und eine Gruppe „notes“ sowie die erforderlichen logischen Laufwerke für Daten und Programme erstellt werden.

Diese Seite ist zur Zeit nicht belegt.

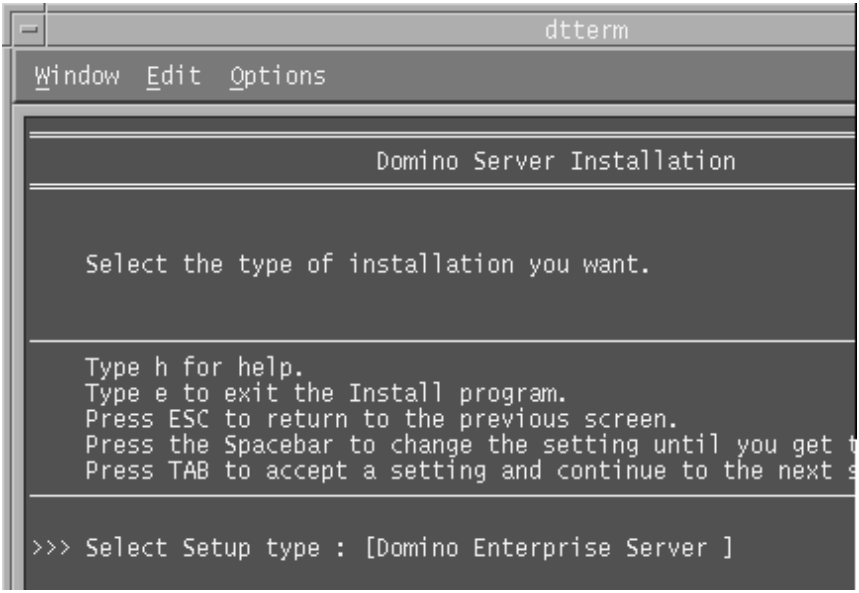
4.3.2 Installation

Die Domino-Installation unter AIX verläuft in den bereits beschriebenen zwei Phasen (Kopieren der Dateien und Konfiguration). Zum Starten des Installationsprozesses wird der Befehl „install“ verwendet.



Installation starten

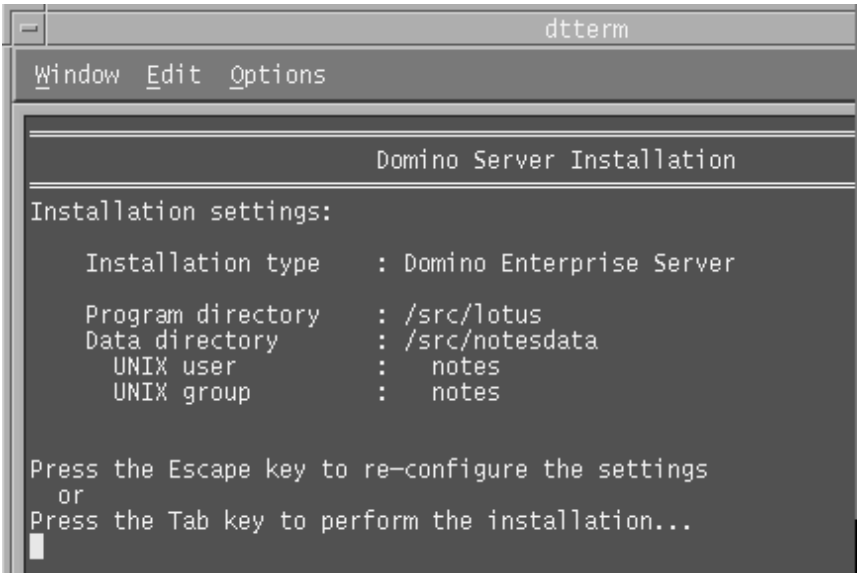
Nach dem Begrüßungsbildschirm und einigen Seiten Lizenzbestimmungen kann der Server-Typ mit Hilfe der Leertaste ausgewählt werden.



Auswahl des Server-Typs

Bei der Auswahl der Verzeichnisse und Programme wird geklärt, ob mehr als ein Domino-Server auf dem System installiert werden sollen. Danach wird zum Benutzer „notes“ und zur Gruppe „notes“ gewechselt. Damit ist der erste Schritt der Installation abgeschlossen.

Es erscheint die Übersicht der Installationsdaten und danach wird die Installation der Dateien durchgeführt. Mit der Abmeldung vom System wird die Installation beendet.



Übersicht der Installationsdaten

Diese Seite ist zur Zeit nicht belegt.

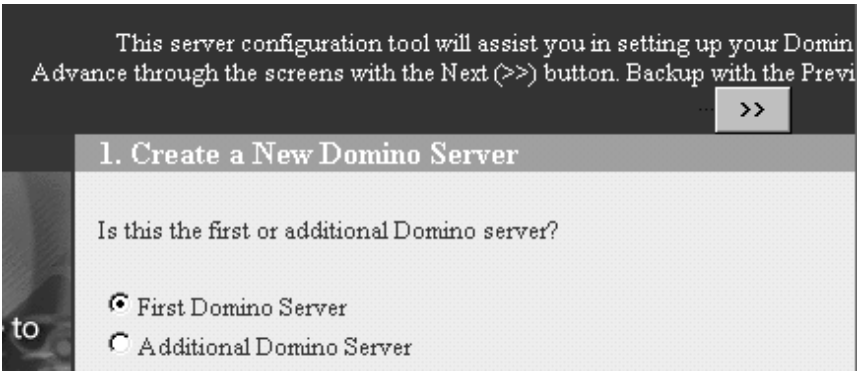
4.3.3 Konfiguration

War das Kopieren der Dateien den übrigen Installationsarten nur ähnlich, so ist die Konfiguration fast identisch. Bevor sie beginnen kann, wird der http-task gestartet.

```
$ /opt/lotus/bin/http httpsetup
01/03/2000 02:49:15 PM  Created new log file as
01/03/2000 02:49:15 PM
************************************************
*      Lotus Domino Server Setup               *
* To setup this server, please connect         *
*     your web browser to port 8081            *
* Example: http://this.server.com:8081         *
************************************************
01/03/2000 02:49:16 PM  JVM: Java Virtual Machi
01/03/2000 02:49:19 PM  HTTP Web Server started
01/03/2000 02:50:27 PM  Addin: Agent message bo
Please wait...
01/03/2000 02:50:28 PM  Addin: Agent message bo
```

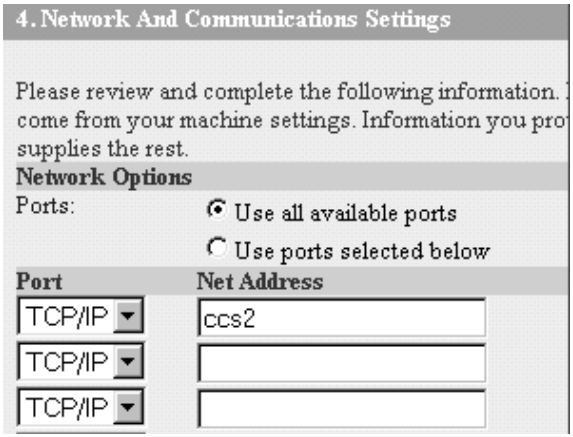
http-task starten

Das System ist jetzt bereit dazu, die Konfiguration über einen Browser einer Arbeitsstation zu starten. Der erste Bildschirm der Konfiguration stellt die Frage nach dem ersten Server der Domäne.



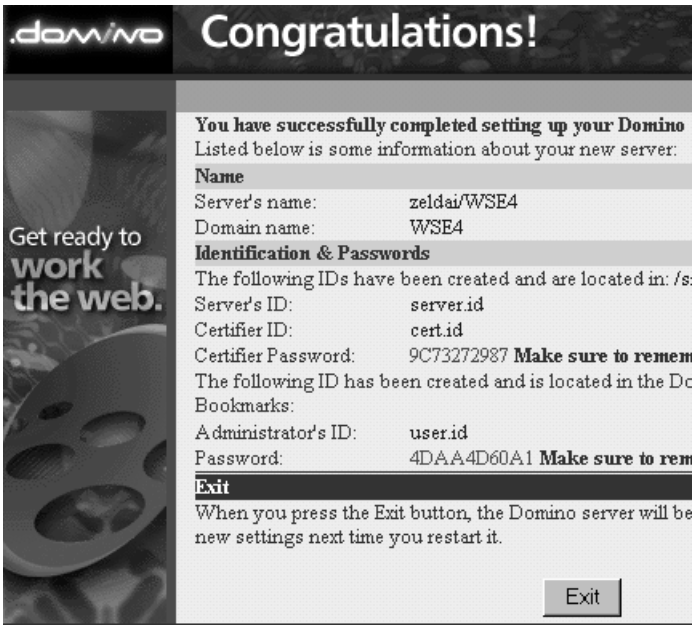
Die erste Seite der Konfiguration

Auch die Folgeseiten sind mit der Windows-Installation identisch. Lediglich auf der Abschlussseite muss mindestens ein Domino-Netzwerk definiert werden.



Netzwerk definieren

Damit ist die Konfiguration abgeschlossen. Die Kennwörter der Abschlussseite sollten an sicherer Stelle hinterlegt werden.



Abschlussseite der Konfiguration

Diese Seite ist zur Zeit nicht belegt.

4.4 Installation eines SMTP-Mail-Servers

Neben dem Notes-eigenen Mail-Protokoll ist der Domino-Server auch in der Lage das SMTP-Protokoll des Internets zu verwenden. e-Mails aus dem Internet empfangen und in das Internet abgeben sind Dienste, die für den SMTP-Prozess des Domino-Servers eingerichtet und mit seiner Hilfe ausgeführt werden können. Bevor ein Domino-Server für das e-Mail-Routing eingesetzt werden kann, müssen eine ganze Reihe von Voraussetzungen geklärt und geregelt werden. Eine wichtige Voraussetzung für den Empfang von e-Mails über SMTP ist z.B. eine feste Adresse, über die der Server im Internet verfügbar ist. Ein im Internet verfügbarer Server stellt natürlich auch ein entsprechendes Sicherheitsrisiko dar, das mit den dafür verfügbaren Instrumenten aufgefangen werden muss. Es ist zu prüfen, welche Firewall, welche Proxy- und/oder Durchgangsserver und welche anderen Einrichtungen verwendet werden sollen. Die Möglichkeiten des Domino-Servers, Sicherheitsrisiken durch entsprechende Einstellungen aufzufangen, sind sehr umfangreich. Welche dieser Möglichkeiten eingesetzt werden, hängt ganz von der Konstellation ab, in der ein Domino-Server eingebunden ist. Damit der SMTP-Server seine Arbeit aufnehmen kann, sind folgende Schritte zu unternehmen:

Februar 2002 / 8. EL

❶❷❸ Ausführungsschritte:

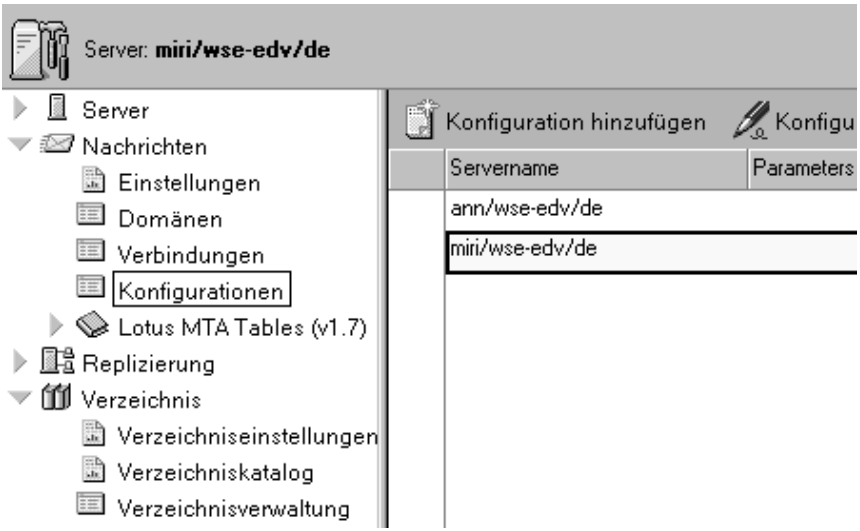
1. Erstellen oder anpassen des Konfigurationsdokumentes für den Server, der als SMTP-Server verwendet werden soll.
2. Erstellen eines Domänen-Dokumentes für eine globale Domäne (falls erforderlich).
3. Anpassung des Serverdokumentes für den SMTP-Server.

❶❷❸

Diese Schritte enthalten eine Reihe von Teilschritten, die im Folgenden beschrieben werden.

4.4.1 Angaben im Server-Konfigurationsdokument

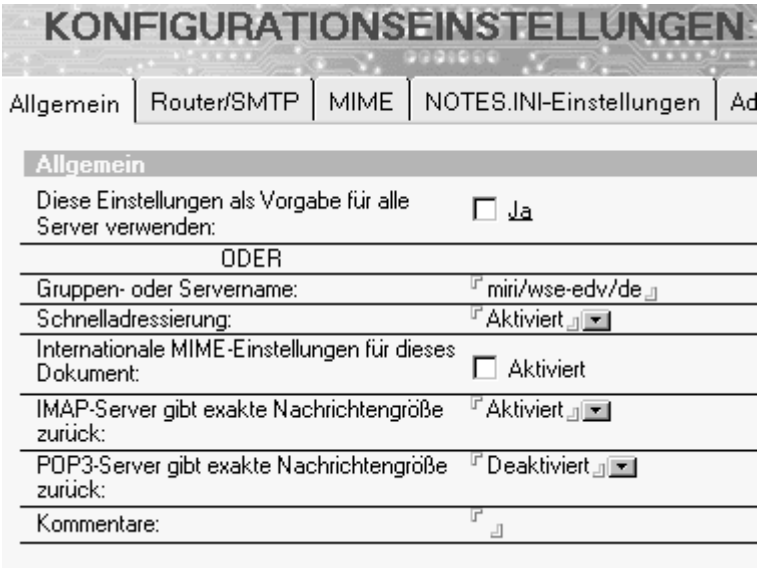
Sollte noch kein Konfigurations-Dokument vorhanden sein, das für den SMTP-Server gilt, so muss eines erstellt werden. Für den SMTP-Prozess sind vor allem Angaben zur Beschränkung des Mail-Eingangs und -Ausgangs erforderlich. Das Konfigurationsdokument eines Servers wird im Administrator-Client unter „Nachrichten / Konfigurationen" aufgelistet. Ein neues Konfigurationsdokument kann mit Hilfe der Schaltfläche „Konfiguration hinzufügen" erstellt werden.



Konfigurationsdokument auswählen

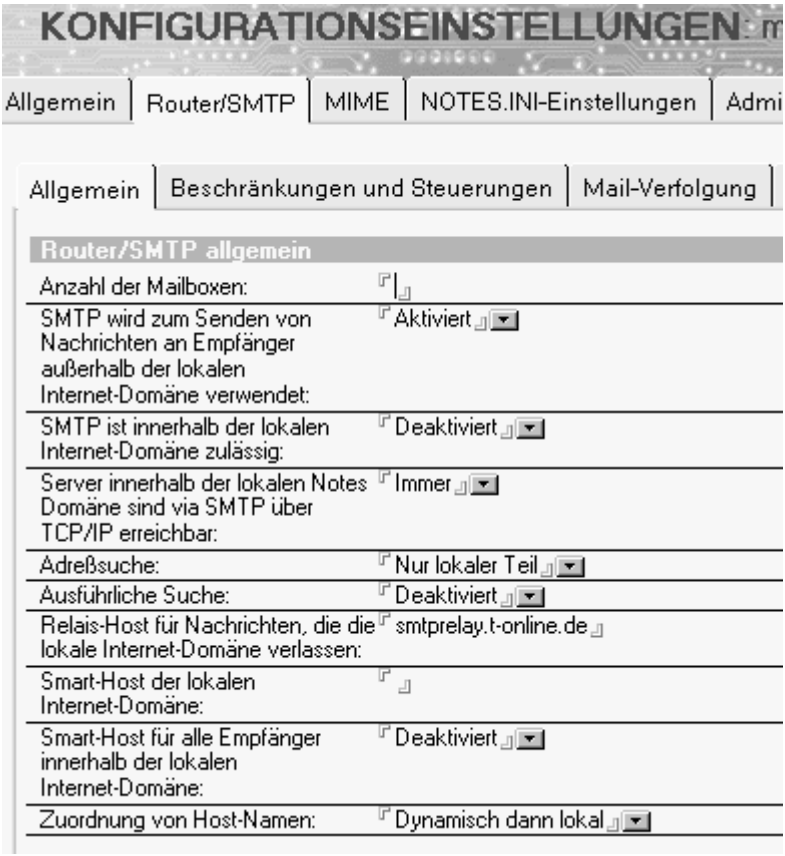
Das geöffnete Konfigurations-Dokument enthält im ersten Register mit dem Titel „Allgemein" Einträge zu seinem Geltungsbereich. Wird das Feld "Diese Einstellungen als Vorgabe für alle

Server verwenden" angekreuzt, so gilt das Dokument für alle Server der Domäne. Wird das Feld "Gruppen- oder Servername" verwendet, so kann mit „*" ebenfalls erreicht werden, dass das Dokument für alle Server der Domäne gilt. In diesem Feld können außerdem Servergruppen oder ein einzelner Server eingetragen werden. Bei der Suche, ob ein Konfigurationsdokument gültig ist, geht der Domino-Server nach dem Prinzip vor, dass spezielle Dokumente Vorrang vor allgemeinen haben. Existiert also ein Konfigurationsdokument für den Server „miri/wse-edv/de" und die Servergruppe „GernanServers", so wird das Dokument des Servers dem der Gruppe vorgezogen, auch wenn der Server Mitglied der Gruppe „GermanServers" ist.



Register "Allgemein" im Konfigurationsdokument

Mit den Angaben zur Mail-Weitergabe und zum SMTP beschäftigt sich das Register „Router / SMTP". Im Unterregister „Allgemein" wird aktiviert, dass SMTP zum Senden von Nachrichten an Empfänger außerhalb der lokalen Internet-Domäne verwendet wird.



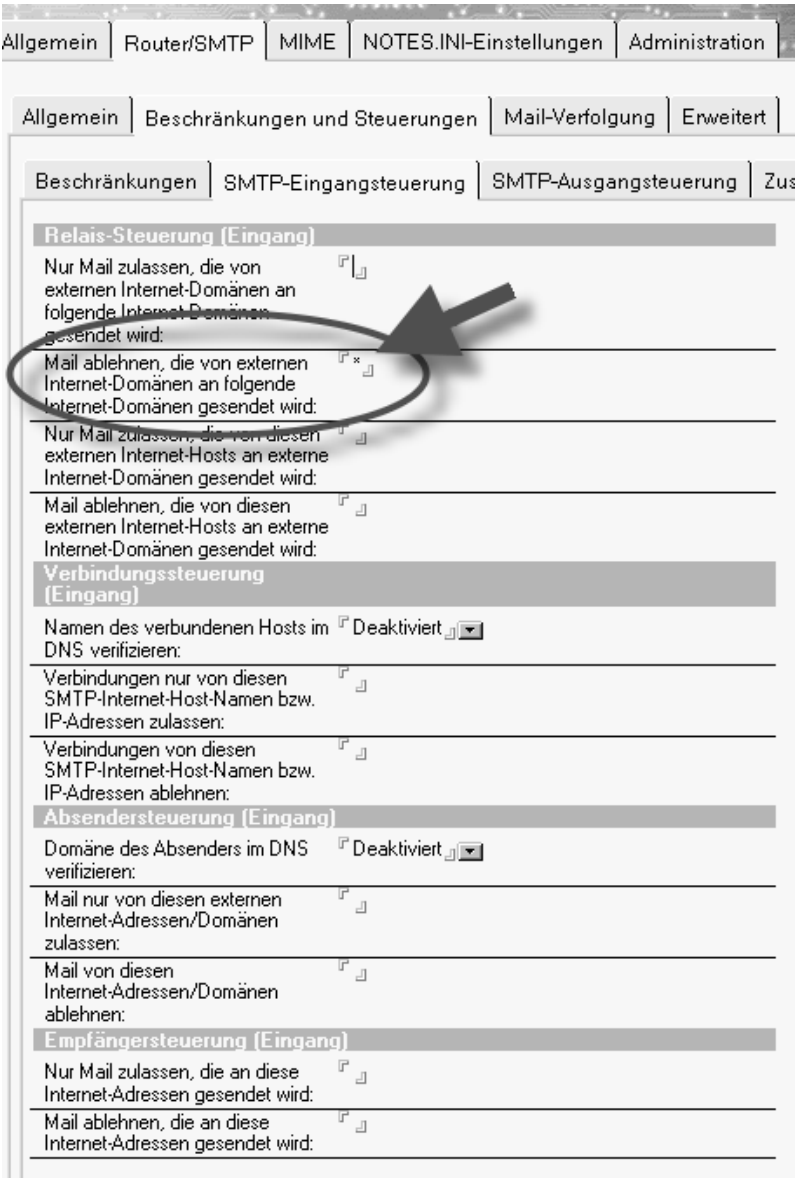
SMTP-Angaben im Konfigurationsdokument

Das Feld „Relais-Host für Nachrichten, lokale Internet-Domäne verlassen" kann (oder muss) verwendet werden, wenn die Adressauflösung der Empfänger-Adresse einer Nachricht nicht vom eigenen Server, sondern von dem angegebenen Relais-Host durchgeführt werden soll. Das kann eine Firewall sein oder ein spezieller Server des Providers. In dem gezeigten Beispiel wird ein Relais-Host von T-Online verwendet, weil T-Online nicht in der Lage ist, Nachrichten an eigene Adressen über die Standard-Mail-Server zuzustellen.

Ein Smart-Host hat ähnliche Funktionen, allerdings im internen Bereich. Hier wird ein Server dazu verwendet generell die Adress-Zuordnung für solche Adressen vorzunehmen, die nicht im Domino-Verzeichnis enthalten sind.

Das Feld „Zuordnung von Hostnamen" bewirkt in der Standard-Einstellung, dass zunächst auf einem DNS und dann erst lokal nach dem Hostnamen gesucht wird. Hat der Server keine Verbindung zu einem entsprechenden DNS sollte der Eintrag auf: "Nur lokale Zuordnung (Host-Datei)" geändert werden.

Im Register „Router / SMTP" ist ein ganzes Bündel an Einschränkungen hinterlegt, die beim Ein- oder Ausgang von SMTP-Nachrichten greifen können. Im Unterregister „SMTP-Eingangssteuerung" ist ein Abschnitt „Relais-Steuerung (Eingang)" zu finden. Der SMTP-Server sendet Nachrichten, die nicht zugeordnet werden können zurück. Diesen Umstand können Außenstehende dazu verwenden, um über einen fremdem SMTP-Server Mails zu versenden.



Beschränkungen

Damit das nicht möglich ist, können diese Felder mit Einträgen gefüllt werden:

- **„Nur Mail zulassen, die von externen Internet-Domänen an folgende Internet-Domäne gesendet wird"**

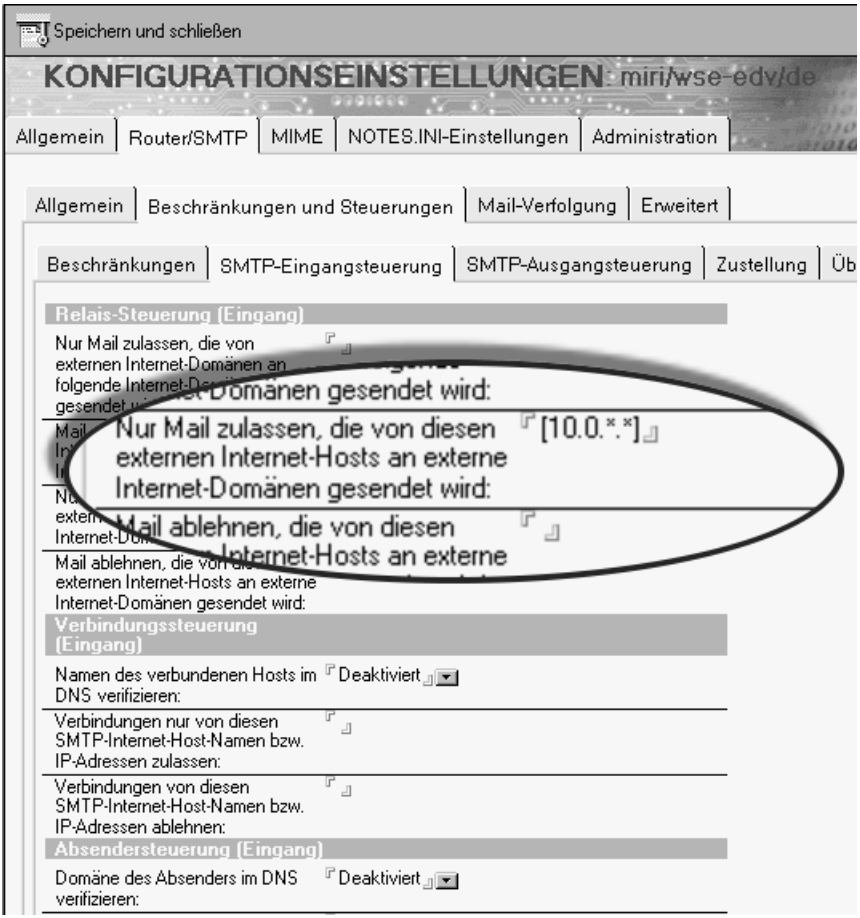
  Hier können eine oder mehrere eigene Domänen eingetragen werden. Mehrere Namen werden durch Komma getrennt. Damit werden alle e-Mails abgelehnt, die nicht an die eigene(n) Domäne(n) gerichtet sind.

- **„Mail ablehnen, die von diesen externen Internet-Hosts an externe Internet-Domänen gesendet wird"**

  Im Normalfall ist es ausreichend, wenn in dieses Feld ein „*" eingetragen wird. Damit wird jeder Mail-Weiterleitungsversuch von außen unterbunden.

- **„Nur Mail zulassen, die von diesen externen Internet-Hosts an externe Internet-Domänen gesendet wird"**

  Der Normalfall wird auch dann durchbrochen, wenn der SMTP-Server auch von MS-Outlook-Clients verwendet werden soll. In diesem Fall stuft der SMTP-Server diese Clients als externe Hosts ein. Eine Weiterleitung wäre also bei der generellen Ablehnung ausgeschlossen. In diesem Fall kann in diesem Feld ein Adressbereich angegeben werden, der die Mail-Weiterleitung erlaubt.



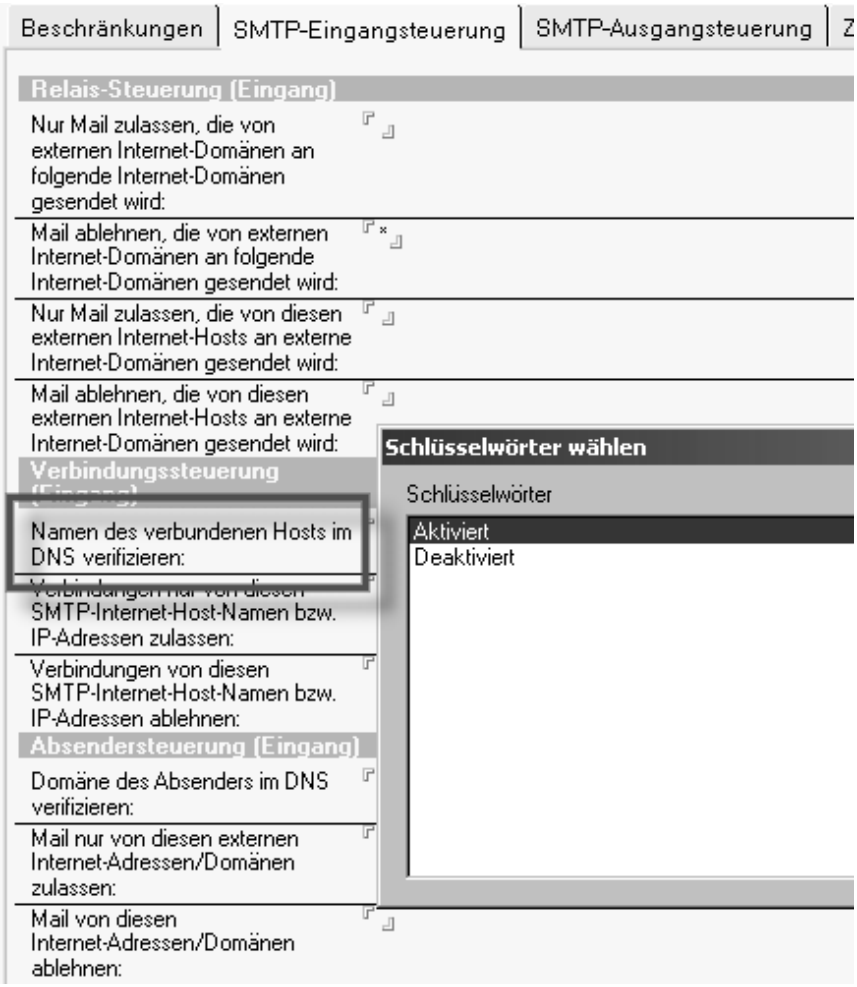
Spezielle externe Hosts zulassen

- **„Mail ablehnen, die von diesen externen Internet-Hosts an externe Internet-Domänen gesendet wird"**

  Ist dieses Feld mit Namen oder IP-Adressen gefüllt, werden alle Mails weitergeleitet, außer denen, die an die genannten Adressen gehen.

Wenn mehr als eines dieser Felder verwendet wird, muss darauf geachtet werden, dass keine Überschneidungen in den Definitionen enthalten sind.

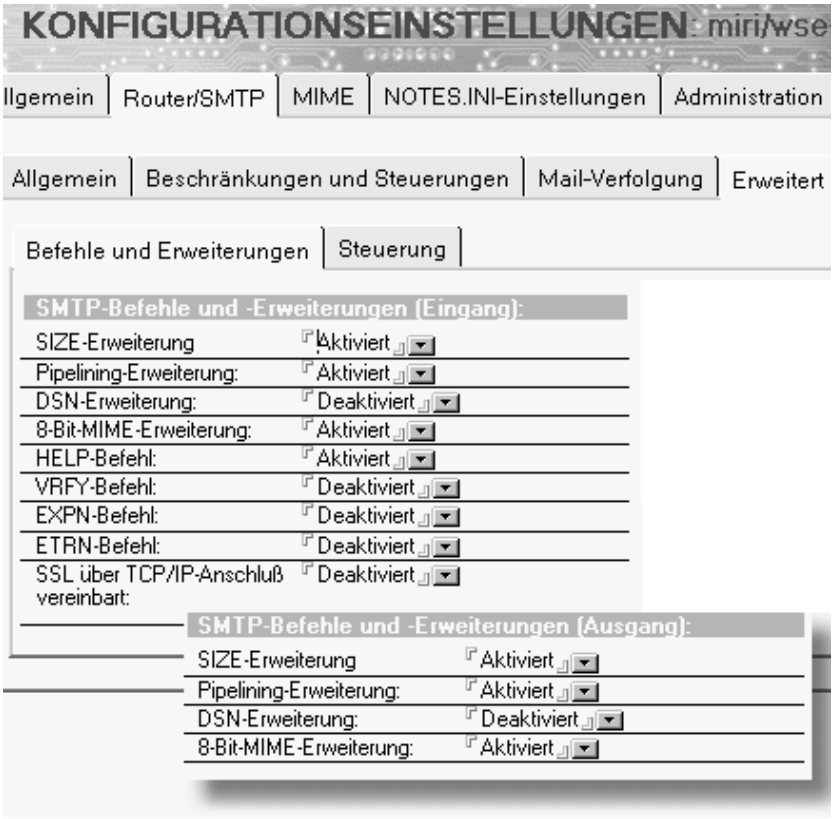
Weitere Beschränkungen sind möglich, aber in der Regel nicht erforderlich. So kann es z.B. sinnvoll sein, nur Mails anzunehmen, die von einer Domäne kommen, die in einem DNS eingetragen ist.



Absenderdomäne verifizieren

Das kann allerdings auch dazu führen, dass Nachrichten im eigenen System nicht mehr zugestellt werden, weil der Absender aus technischen Gründen mit einem speziellen Domänen-Namen arbeitet.

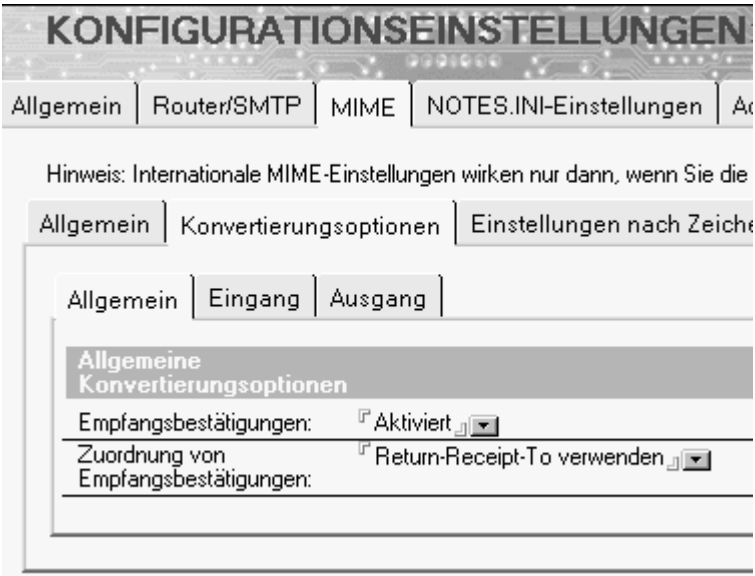
Ein sinnvoller Eintrag befindet sich im Unterregister „Erweitert" des Registers „Router / SMTP". Es handelt sich um das Feld „8-Bit-Mime aktivieren".



8-Bit-Mime aktivieren

Diese Aktivierung sollte sowohl für den Nachrichten-Eingang als auch den -Ausgang erfolgen.

Unter dem Register „Mime" kann eine Angabe zu der Ausführung von Empfangsbestätigungen gemacht werden. Dazu wird im Unterregister „Allgemein" das Feld Empfangsbestätigungen auf „Aktiviert" gesetzt.



Empfangsbestätigungen

Das ist erforderlich, wenn Empfangsbestätigungen an Mail-Absender erlaubt sein sollen. Das Feld Zuordnung von Empfangsbestätigungen enthält zwei Möglichkeiten zur Auswahl:

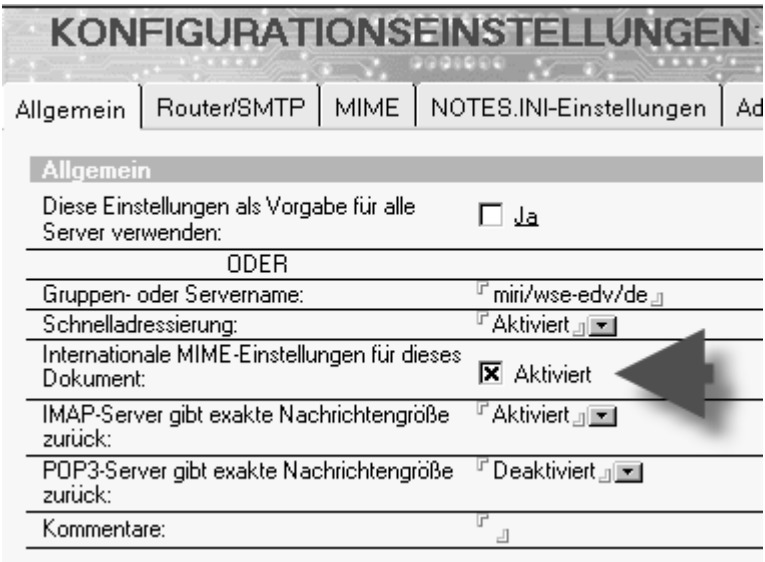
- **Disposition-Notification-To**

  Der Empfang wird bestätigt, wenn die e-Mail auf dem Server eingegangen ist.

- **Return-Receipt-To**

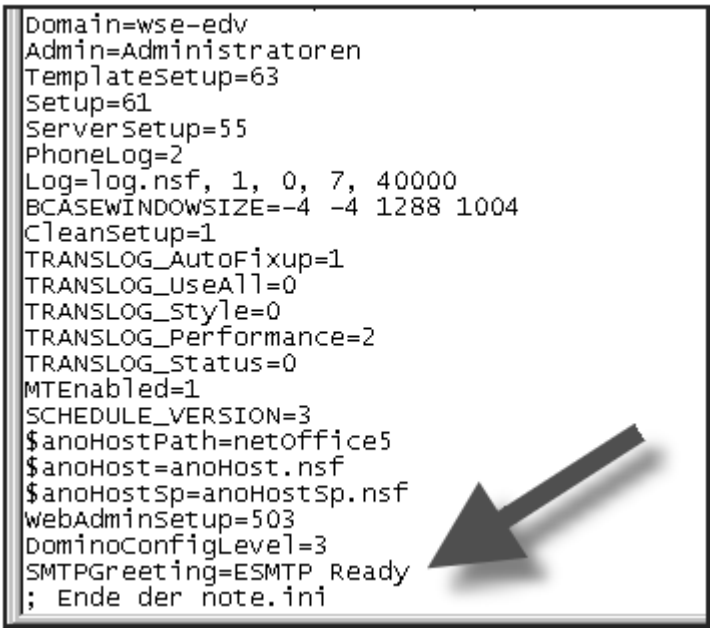
  Der Empfang wird bestätigt, wenn die Nachricht beim Empfänger eingegangen ist.

Alle Einträge zur Steuerung des MIME-Formates werden nur wirksam, wenn im Register „Allgemein" des Konfigurationsdokumentes das Feld „Internationale MIME-Einstellungen für dieses Dokument Aktiviert" angekreuzt wird.



MIME-Einstellungen aktivieren

Wer verhindern will, dass sich der SMTP-Server im Internet als Domino-Server mit dem aktuellen Release-Stand zu erkennen gibt, kann über einen speziellen Eintrag in der Datei „Notes.ini" einen eigenen Kennsatz definieren.



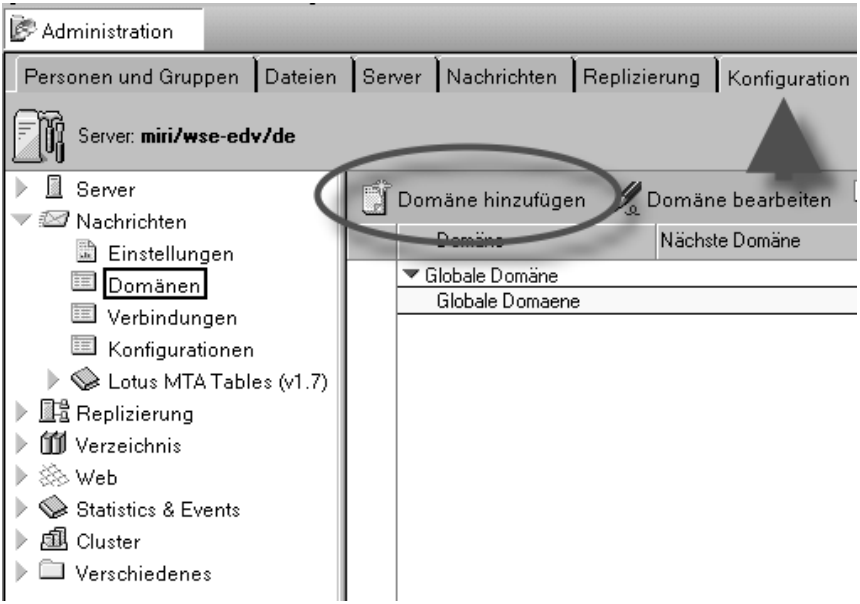
Eintrag in der Ini-Datei des Servers

Dazu wird der Eintrag „SMTGreetings" mit dem gewünschten Kennsatz versehen (z.B. WESMTP Ready").

Diese Seite ist zur Zeit nicht belegt.

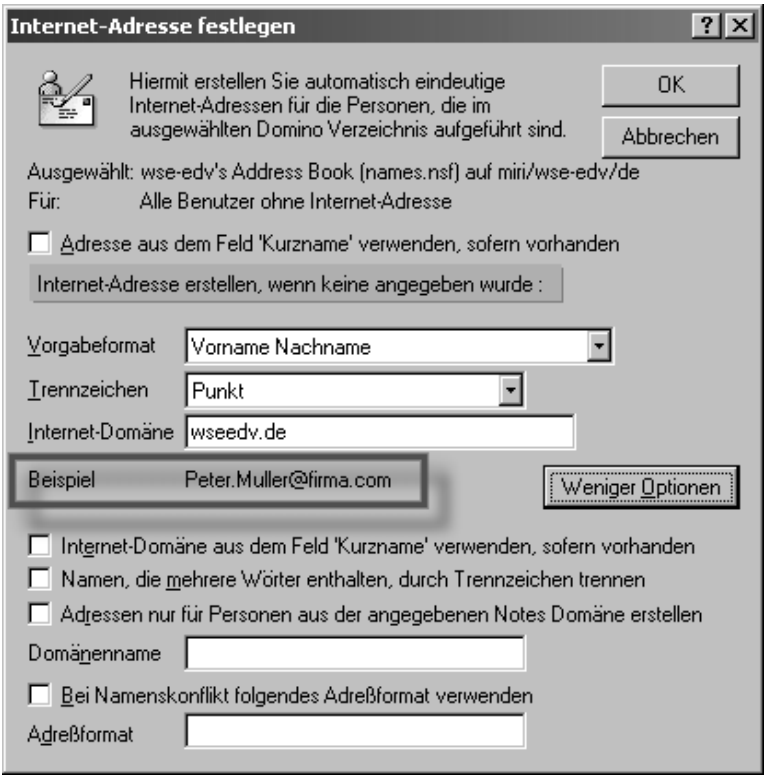
4.4.2 Das globale Domänen-Dokument

Das globale Domänendokument dient dazu, einen Internet-Domänennamen mit dem Namen einer Notes-Domäne zu verknüpfen. Außerdem enthält es Angaben zur Zusammensetzung der e-Mail-Adresse, die für einen Notes-Benutzer nach außen gegeben wird. Um ein solches Dokument anzulegen wird im Administrator-Client unter dem Register „Konfiguration" im seitlichen Gliederungsmenü die Position „Nachrichten" und darunter „Domänen" ausgewählt. Ist noch kein globales Domänen-Dokument vorhanden, kann es mit Hilfe der Schaltfläche „Domäne hinzufügen" erstellt werden.



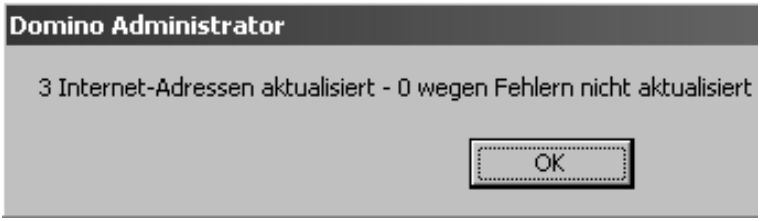
Domäne hinzufügen

Wird in allen Personendokumenten eine Internetadresse hinterlegt, so kann im globalen Domänendokument auf die Regeln zur Adressbildung verzichtet werden. Um nicht jedes Personendokument bearbeiten zu müssen, kann mit Hilfe des Administrator-Clients ein generelles Format für Internet-Adressen definiert und in die Personendokumente eingefügt werden. Dazu findet man im Register „Personen und Gruppen" bei den Werkzeugen eine Position mit dem Namen: „Internet-Adresse festlegen". Wird die Position ausgewählt, so erscheint der Dialog:



Internetadresse festlegen

Die Durchführung dieser Änderung wird mit einer Prompt-Meldung bestätigt.

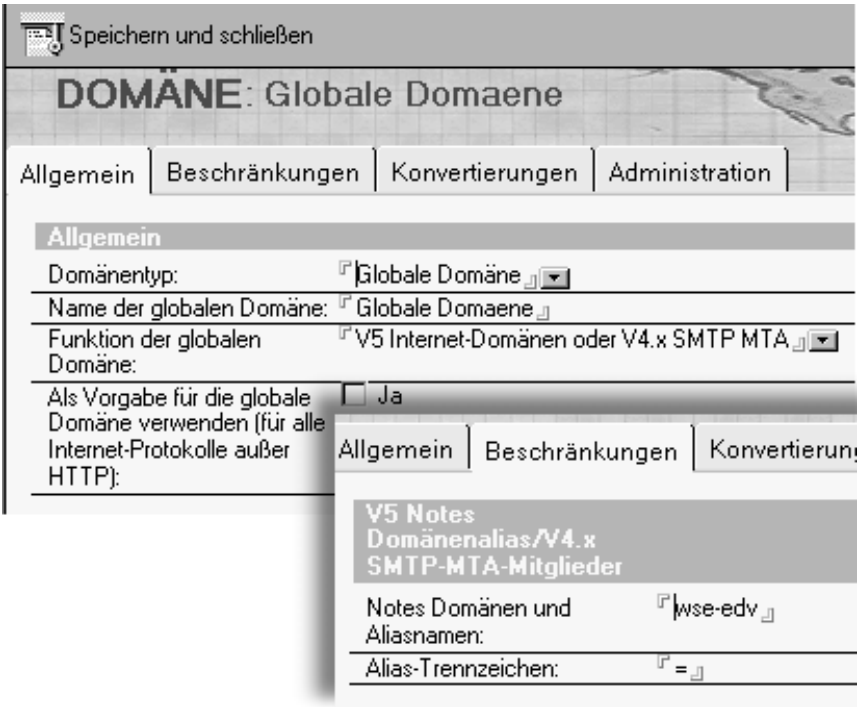


Bestätigung für die Änderung der Personendokumente

Diese Möglichkeit der generellen Erstellung von Internetadressen besteht erst seit R5.

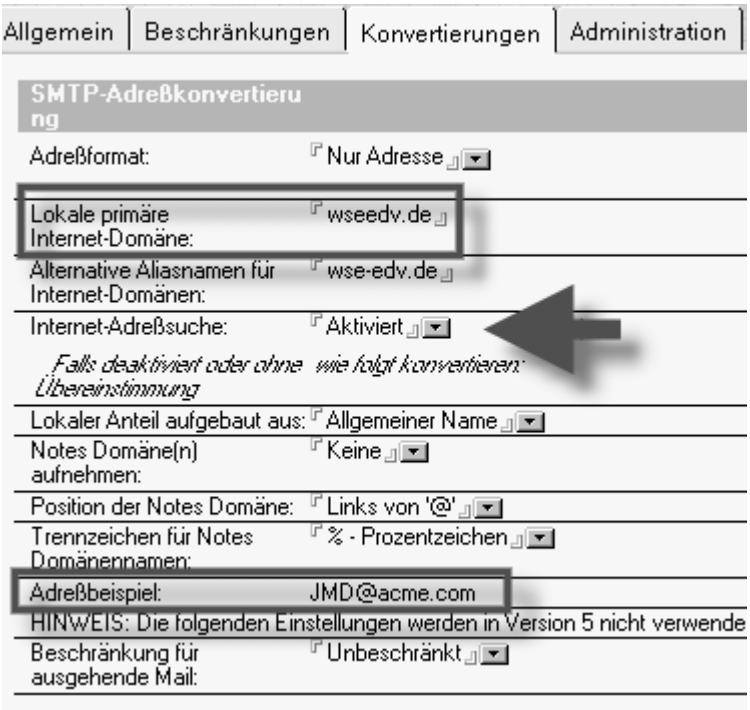
Bei der Erstellung des globalen Domänen-Dokumentes sind nur wenige Dinge zu beachten. Der Name ist nur dann von Bedeutung, wenn mehrere globale Domänen-Dokumente zum Einsatz kommen. Das wird benötigt, wenn sich der Name des Unternehmens geändert hat oder mehrere Internet-Domänen verwendet werden.

In diesem Fall, kann über den „Notes.ini"-Eintrag „SERVER_DEFAULT_GLOBAL_DOMAIN" gesteuert werden, welches globale Domänendokument ein bestimmter Server verwenden soll.



Globale Domäne definieren

Die wichtigsten Angaben werden im Register „Konvertierungen" gemacht, weil hier die Internet-Absender-Adresse aus dem Notes-Namen der Benutzer definiert wird.



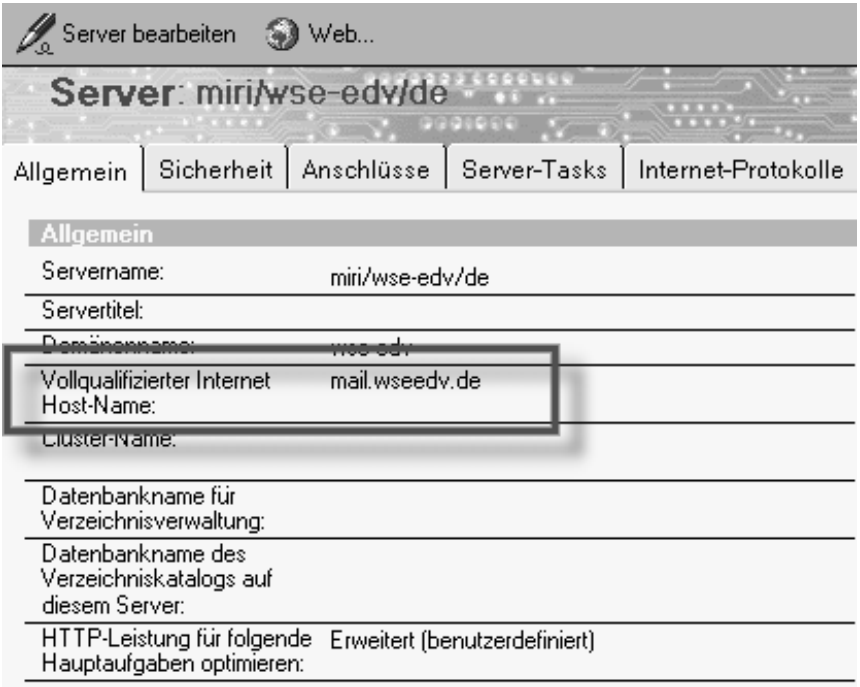
Konvertierungsangaben

Zusätzlich zu der Angabe der Internet-Domäne wird die Internet-Adresssuche aktiviert. Im Adressbeispiel kann das Aussehen der Adresse nachgesehen werden, wenn die Adresssuche nicht aktiviert und der Name nach den darunter stehenden Regeln gebildet werden soll.

Diese Seite ist zur Zeit nicht belegt.

4.4.3 Einträge im Server-Dokument

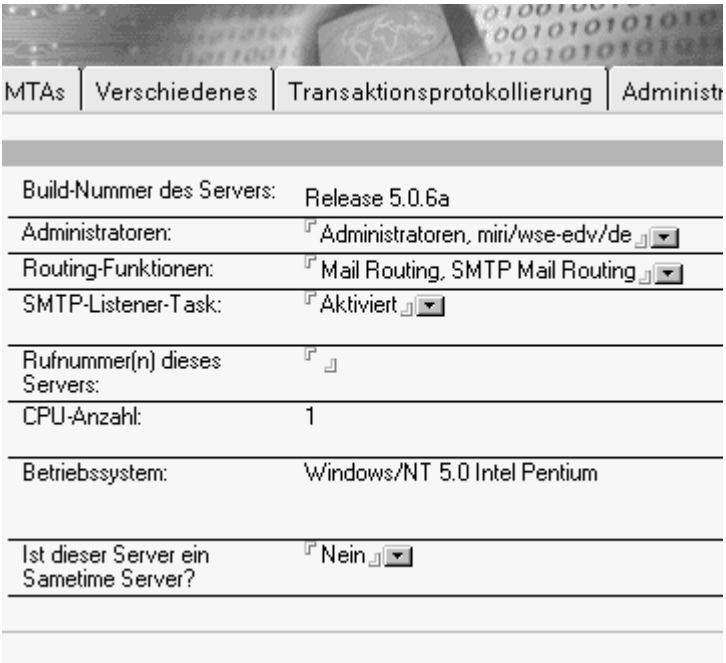
Damit der SMTP-Server seine Arbeit aufnehmen kann, müssen noch einige Einträge im Server-Dokument dieses Servers vorgenommen werden.



Internet Host-Name

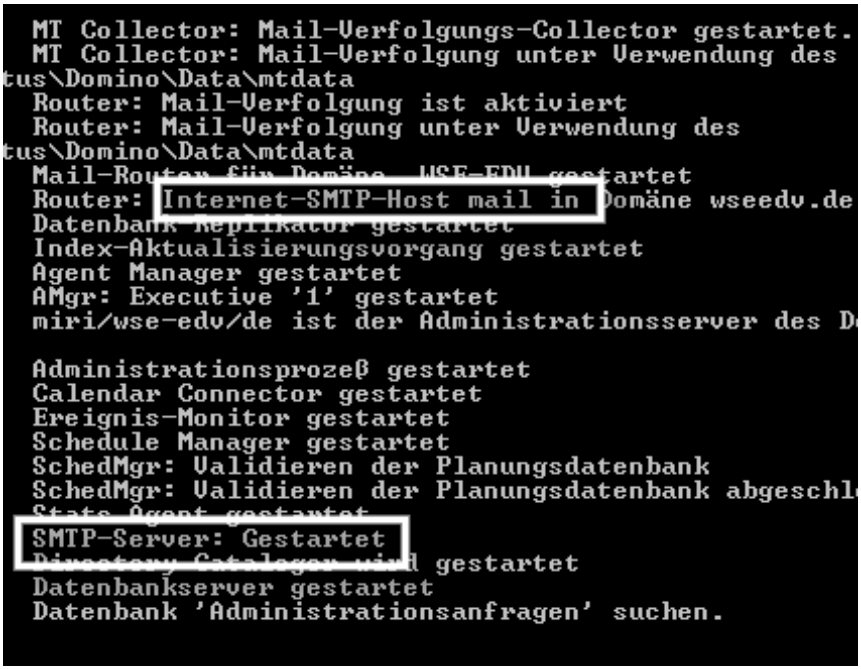
Der erste Eintrag ist der „Vollqualifizierte Internet Host-Name", mit dem der Server im Internet erreichbar ist.

Außerdem wird die SMTP-Routing-Funktion des Servers in die Routing-Funktionen aufgenommen.



SMTP im Server-Dokument

Und zum Schluss wird auch der SMTP-Listener-Task aktiviert. Jetzt wird der Server neu gestartet. An der Konsole kann verfolgt werden, wie die SMTP-Prozesse gestartet werden.



SMTP-Prozesse

Sind alle Einträge richtig vorgenommen, werden die Mails an der Konsole angezeigt und den Empfängern zugestellt.

Diese Seite ist zur Zeit nicht belegt.

4.5 Konfiguration eines Domino IMAP-Servers

Die Verarbeitung von eingehenden e-Mails kann in Lotus Notes durch die Verwendung unterschiedlicher Internet-Protokolle realisiert werden. Neben der Unterstützung des populären POP3 (**P**ost **O**ffice **P**rotocol) wird in Domino auch das Internet-Mail-Protokoll IMAP4 (**I**nternet **M**ail **A**ccess **P**rotocol) unterstützt. Die Unterstützung von IMAP ist ab der Domino-Release-Version 5 verfügbar.

Der POP3-Dienst, auf dessen Grundfunktionen der IMAP4-Dienst basiert und aufsetzt, wurde entwickelt, um Internet e-Mails für Clients auf Internet-Servern nach einem Standard zur Verfügung zu stellen und diese auf den Client zu übertragen.

Es wird davon ausgegangen, dass die e-Mails auf dem Server gesammelt bzw. zwischengespeichert werden, um dann über einen e-Mail-Client von dem Server für die weitere Verarbeitung heruntergeladen zu werden.

Unter Verwendung des Protokolls IMAP4 werden diverse Funktionen, die unter POP3 auf dem Client durchgeführt werden, auf den Server verlagert. Der Hauptunterschied zu POP3 liegt darin, dass unter Verwendung von IMAP im Normalfall die e-Mails nicht auf dem Client gespeichert werden, sondern auf dem Mail-Server bleiben.

Dies hat eine Verringerung der Plattenauslastung der Clients und im Gegensatz dazu einen höheren Plattenplatzbedarf auf dem Ser-

ver zur Folge – für den Einsatz in einer Domino-Umgebung durchaus eine interessante Alternative zur Verwendung des POP3-Protokolls.

IMAP in einer Domino-Umgebung setzt nicht voraus, dass die e-Mails ausschließlich auf dem Server gespeichert sind; bei Bedarf können diese auch auf den Client übertragen werden.

Der IMAP-Dienst ist in Form einer Schnittstelle realisiert, die die Kommunikation zwischen IMAP-Mail-Clients und dem Domino-Mail-Server übernimmt.

Für die Nutzung der IMAP-Funktionen müssen für jeden Benutzer ein Personendokument im Verzeichnis und eine zugeordnete Mail-Datei vorhanden sein. Sollen verschlüsselte Mails verarbeitet werden, dann sind zusätzlich eine Notes ID und eine Registrierung des Benutzers notwendig.

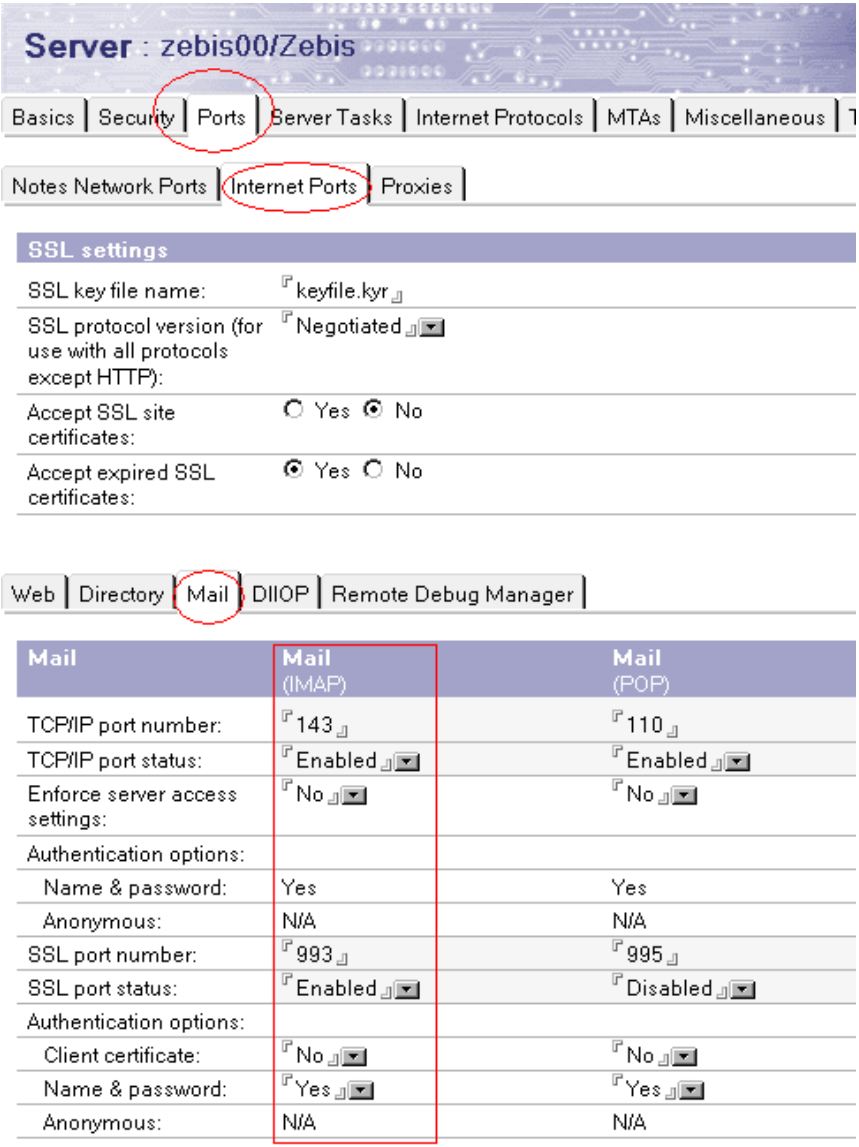
Bevor mit einer Notes-Mail-Datei IMAP genutzt werden kann, muss die Mail-Datei zunächst angepasst und auf die IMAP-Anforderungen abgestimmt werden. Die Umstellung der Mail-Dateien kann mit dem Befehl „*convert*“ oder automatisch bei der Umstellung des Servers auf IMAP durchgeführt werden.

Die Anmeldung bei IMAP erfolgt in den Standardeinstellungen unverschlüsselt über den Benutzernamen mit dem dazugehörigen Kennwort. Es empfiehlt sich in jedem Fall auch bei der Nutzung von IMAP die Verwendung der SSL-Verschlüsselung.

4.5.1 Konfiguration eines IMAP-Servers

Der IMAP-Server kommuniziert in der Standardkonfiguration über den TCP/IP Port 143.

Die Anpassungen können mittels des Domino-Administrators im Server-Dokument vorgenommen werden. Unter dem Register „Ports/Internet Ports/Mail“ können die Einstellungen sowohl für POP3 als auch für IMAP durchgeführt werden.



Server : zebis00/Zebis

Basics | Security | Ports | Server Tasks | Internet Protocols | MTAs | Miscellaneous

Notes Network Ports | Internet Ports | Proxies

SSL settings

SSL key file name:	keyfile.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	○ Yes ◉ No
Accept expired SSL certificates:	◉ Yes ○ No

Web | Directory | Mail | DIIOP | Remote Debug Manager

Mail	Mail (IMAP)	Mail (POP)
TCP/IP port number:	143	110
TCP/IP port status:	Enabled	Enabled
Enforce server access settings:	No	No
Authentication options:		
Name & password:	Yes	Yes
Anonymous:	N/A	N/A
SSL port number:	993	995
SSL port status:	Enabled	Disabled
Authentication options:		
Client certificate:	No	No
Name & password:	Yes	Yes
Anonymous:	N/A	N/A

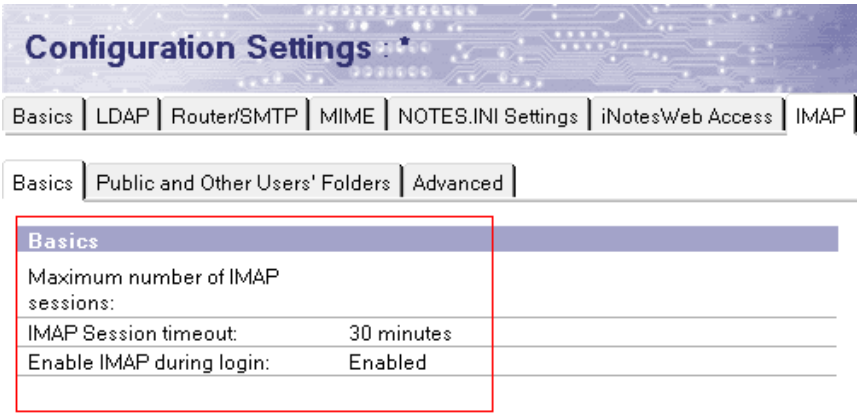
IMAP-Serverdokument

Die Verwendung der TCP/IP-Ports ist im Standard wie folgt zugewiesen und sollte nur in Ausnahmefällen verändert werden:

- POP3: Port 110
- IMAP unverschlüsselt: Port 143
- IMAP verschlüsselt (SSL): Port 993

Kann mit den Standardports nicht gearbeitet werden, dann ist zu beachten, dass Anpassungen an den Ports auf dem Server und auf jedem Client durchgeführt werden müssen!

Im Konfigurationsdokument des Servers können unter „*IMAP/ Basics*“ weitere Einstellungen für die IMAP-Konfiguration vorgenommen werden:



IMAP-Details

- Maximum number of IMAP sessions
  - Legt die maximale Zahl paralleler IMAP Sitzungen fest.
  - Dieser Parameter entspricht in Release 5 dem notes.ini-Eintrag „*IMAPMaxSessions*“.

- IMAP Session timeout
  - Dauer in Minuten, die eine interaktive Sitzung online bleibt.
  - Dieser Parameter entspricht in Release 5 dem notes.ini-Eintrag „*IMAP_Session_Timeout*“.

- Enable IMAP during login
  - Automatische Konvertierung von Mail-Daten nach Umstellung der Mail-Datenbank auf IMAP. Wurde eine Mail-Datenbank umgestellt und ist dieser Parameter „disabled“, dann muss vor der ersten Nutzung mit IMAP eine manuelle Umstellung mit „convert“ durchgeführt werden. Steht der Parameter auf „*enabled*“, dann wird beim nächsten Öffnen der Datenbank die Umstellung automatisch aufgerufen. Wurde eine Mail-Datenbank nach einer Umstellung nicht konvertiert, dann lässt diese sich nicht öffnen und eine Fehlermeldung wird ausgegeben.

6

Das Domino-Verzeichnis

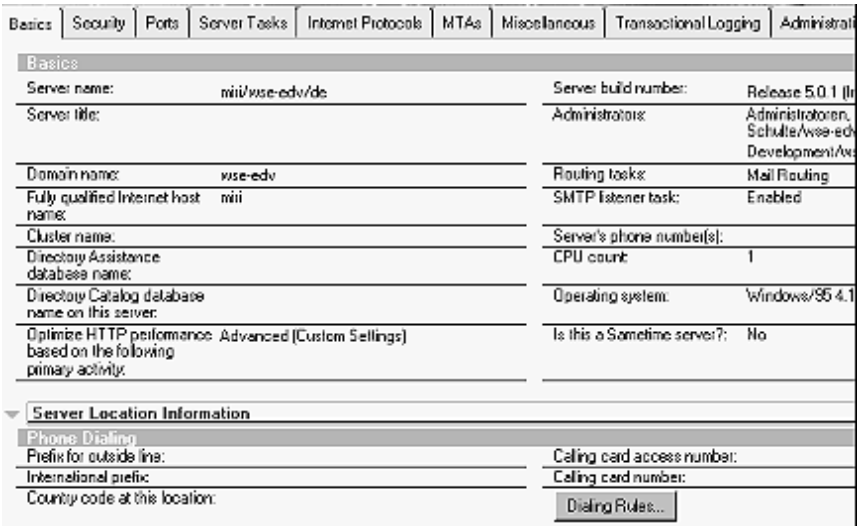
Das Domino-Verzeichnis ist das Herzstück einer Domino-Domäne. Es handelt sich dabei um die Datenbank names.nsf auf dem ersten Server der Domäne. Das Domino-Verzeichnis bietet dem System Auskünfte über Personen, Gruppen und Server der Domäne. Es beinhaltet aber auch Dokumente, die wichtige Parameter für die Server-Prozesse zur Verfügung stellen.

Das wichtigste Dokument in diesem Zusammenhang ist das Server-Dokument. Daneben findet man hier Verbindungsdokumente, Konfigurationen, Programme und externe Domänen.

Server-Dokumente im Administrator-Client

6.1 Das Server-Dokument

Das Server-Dokument ist in eine ganze Reihe von Abschnitten aufgeteilt, die als Register dargestellt sind. In den Abschnitten sind dann wieder Angaben zu den entsprechenden Themen hinterlegbar.



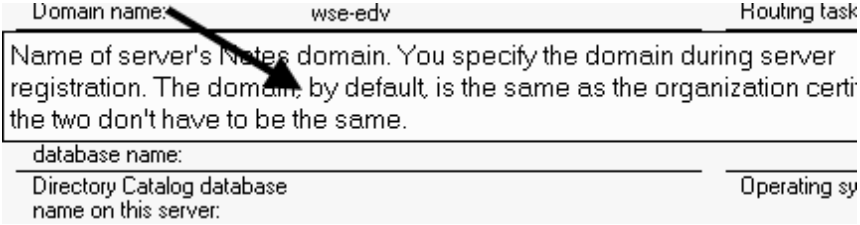
Das Server-Dokument

Wir wollen die einzelnen Abschnitte durcharbeiten. Leider ist es hier aber nicht möglich, wirklich jedes einzelne Feld mit all seinen möglichen Inhalten und Wirkungen aufzuführen.

Diese Seite ist zur Zeit nicht belegt.

6.1.1 Das Register „Allgemein“

Die Grundeigenschaften des ersten Servers der Domäne sind im Abschnitt „Allgemein“ definiert. Zu den einzelnen Feldern erhält man einen Pop-Up-Hilfetext, wenn man den Cursor auf die Feldbezeichung setzt und kurze Zeit die linke Maustaste gedrückt hält.



Pop-Up-Hilfe

Zur Identifikation des Servers dienen die Felder:

- Server-Name

  Eindeutiger Name des Servers, der bei der Installation automatisch angelegt wird.

- Titel

  Nähere Beschreibung des Servers.

- Name der Domäne

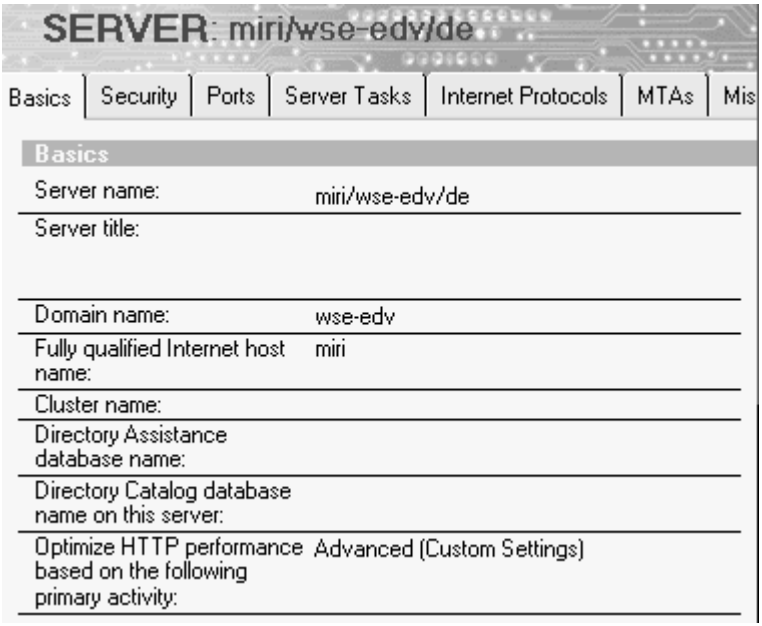
  Auch dieses Feld wird automatisch bei der Installation erstellt und sollte normalerweise nicht geändert werden.

- Internet-Server-Name

  Ist der Server über das Internet erreichbar, so ist hier der Name des Servers für das Internet einzutragen.

- Datenbank für Verzeichnisverwaltung

  Spezielle Datenbank, die dazu dient, die Adressen mehrerer Domänen für die e-Mail-Adressierung zur Verfügung zu stellen.



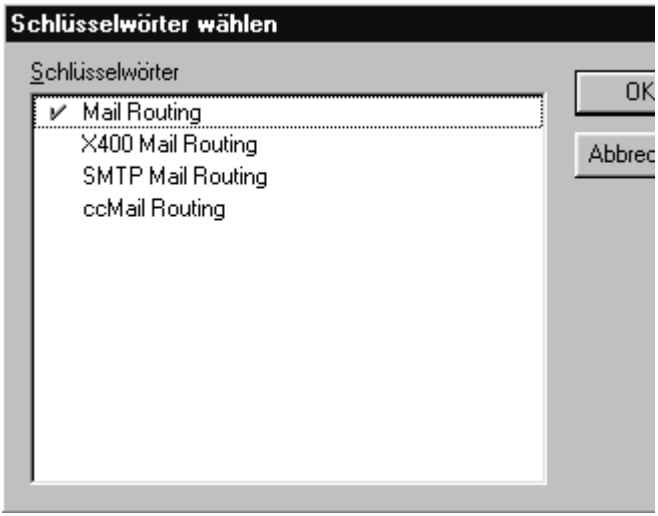
Felder des Server-Dokuments

- Administratoren

  Nur Personen (oder Gruppen), die hier eingetragen sind, dürfen den Server bearbeiten.

- Routing-Funktionen

  Mail-Routing oder auch Routing anderer Mail-Systeme



Mail-Funktionen

- SMTP-Listener-Task

  Aktivieren oder Deaktivieren des SMTP-Prozesses.

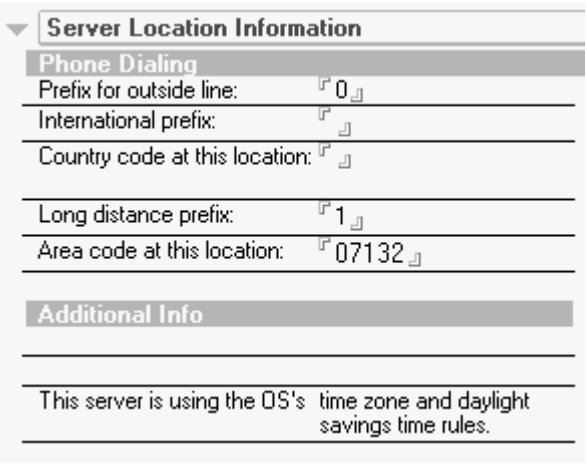
- Telefonnummer des Servers

Server build number:	Release 5.0.1 (Intl)
Administrators:	Administratoren, miri/wse-edv/de, Werner Schulte/wse-edv/de, Development/wse-edv/de
Routing tasks:	Mail Routing
SMTP listener task:	Enabled
Server's phone number(s):	
CPU count:	1
Operating system:	Windows/95 4.10 Intel Pentium
Is this a Sametime server?:	No

Register „Allgemein“ des Server-Dokuments

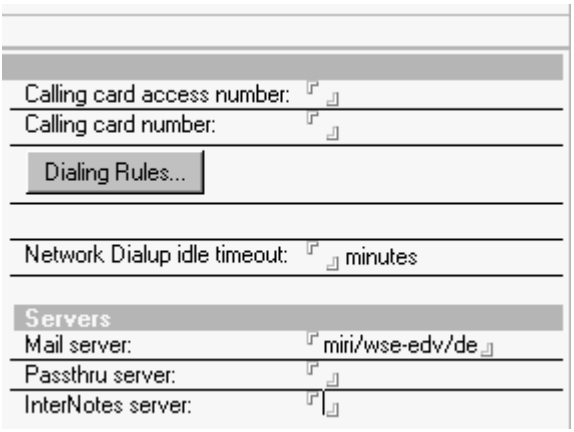
Mit den Angaben zur Arbeitsumgebung des Servers sind drei weitere Gruppen mit Feldern zu definieren.

Die Telefonangaben werden für Vorgabewerte verwendet.



Telefonvorgaben und Zeitzone

Die weiteren Informationen enthalten die Angabe über die gewählte Zeitzone. Die günstigste Variante für die Zeitzone ist in der Regel die des Betriebssystems.



Server

Im Abschnitt „Server“ können Server mit speziellen Aufgaben definiert werden:

- Mail-Server

  Normalerweise ist das der Server selbst.

- Durchgangs-Server

  Falls die Verbindung zu anderen Servern über einen Durchgangs-Server erfolgt.

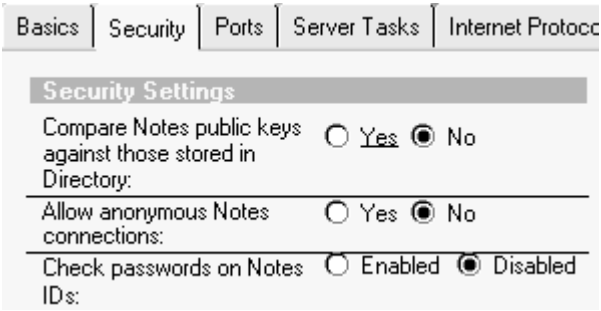
- InterNotes-Server

  Verbindungs-Server zum Internet für die persönlichen Web-Navigatoren der Benutzer.

Diese Seite ist zur Zeit nicht belegt.

6.1.2 Das Register „Sicherheit“

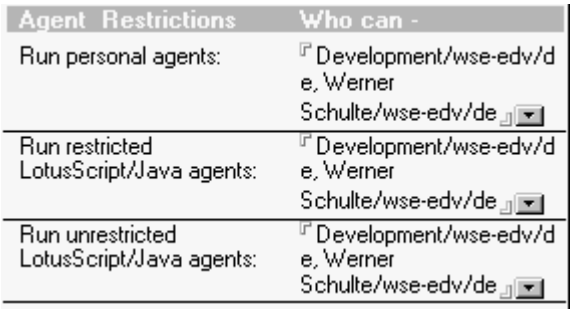
Die Sicherheitseinstellungen beziehen sich auf das Domino-System, aber auch auf Verbindungen zum Internet. Die Grundeinstellungen legen fest, wie ein Zugriff auf den Server geprüft werden soll.



Das Register „Sicherheit“

Im Abschnitt „Server-Zugriff“ wird geregelt, wer auf den Server zugreifen, neue Datenbanken und Repliken anlegen und den Server über einen Browser administrieren darf.

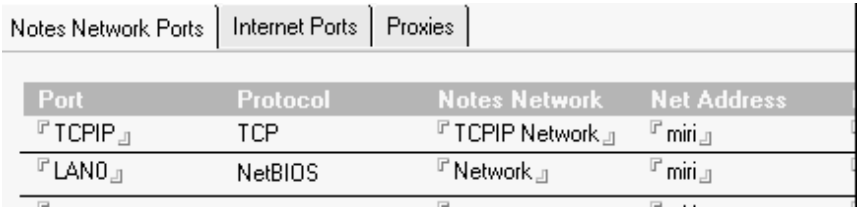
Der Abschnitt für Einschränkungen in Bezug auf das Starten von Agenten muss in jedem Fall gefüllt werden, wenn Agenten auf dem Server laufen sollen. Sind die Felder nicht gefüllt, hat niemand das Recht, Agenten zu starten.



Starten von Agenten

6.1.3 Das Register „Anschlüsse“

Anschlüsse definieren Verbindungen mit dem Server über DFÜ oder Domino-Netzwerke. Aus den verfügbaren Anschlüssen und Netzwerken werden diejenigen ausgewählt, über die der Server erreichbar sein soll.



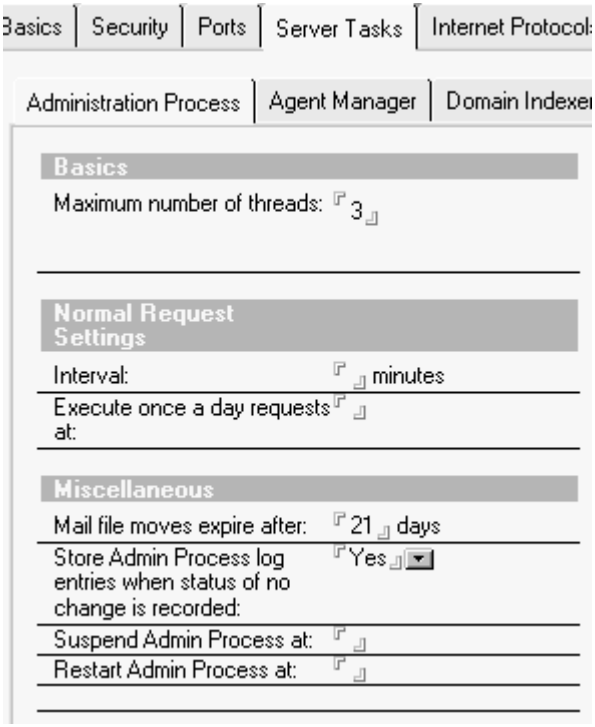
Anschlüsse

Weitere Definitionen betreffen den Internet-Zugang über SSL (Secure Sockets Layer) und die Kommunikation über Proxy-Server.

Diese Seite ist zur Zeit nicht belegt.

6.1.4 Das Register „Server Tasks“

Der Domino-Server arbeitet über verschiedene Prozesse, die aktiv sein können, solange der Server arbeitet. Im Register „Server Tasks“ finden sich viele Einstellungen, die den Ablauf der Prozesse steuern.



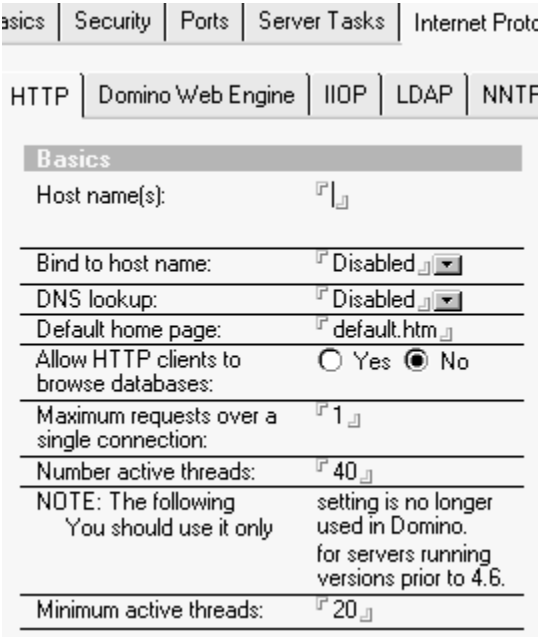
Ausschnitt aus dem Register „Server Tasks“

Das Register unterteilt sich in Unterregister für die Prozesse:

- Administrator-Prozess (Adminp)
- Agenten-Manager
- Index für die Suche über die ganze Domäne hinweg
- Verzeichnis Adressen-Katalog
- Internet Cluster Manager
- Web-Retriever

6.1.5 Das Register „Internet-Protokolle“

Über die Einträge in diesem Register legt man fest, wie auf das Internet zugegriffen wird.



Internet-Protokolle

Die große Anzahl von Parametern wird in Unterregister aufgeteilt:

- HTTP
- Domino Web-Server
- IIOP

- LDAP
- NNTP

Wer seinen Domino-Server als Web-Server betreiben oder ihn im Intranet zur Verfügung stellen will, muss diese Eintragungen genau überprüfen.

6.1.6 Das Register „MTAs“

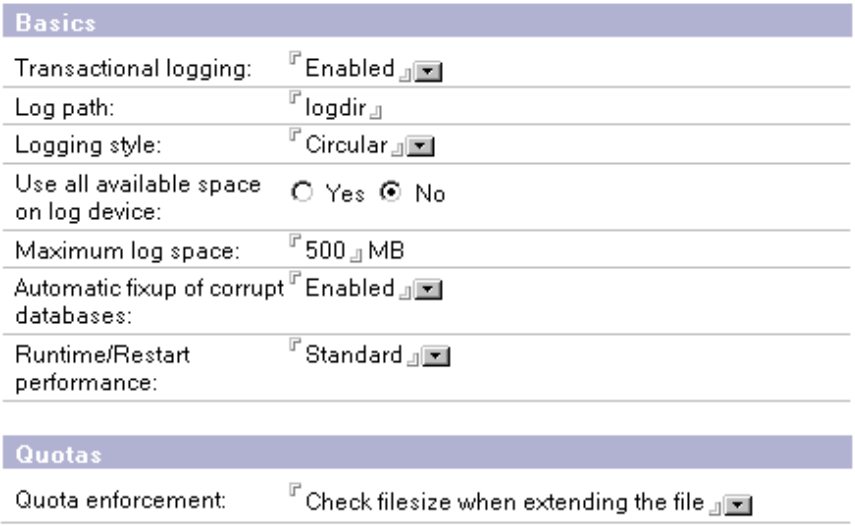
Da der Domino-Server seit Release 5.0 einen eigenen SMTP-Prozess enthält, wird kein MTA (Message Transfer Agent) mehr benötigt. In diesem Register werden die Parameter für Nachrichten über einen Release 4.6 (oder früher) Domino SMTP-MTA, X.400-MTA oder ccMail-MTA gesetzt.

Diese Seite ist zur Zeit nicht belegt.

6.1.7 Das Register „Transaktionsprotokoll“

Transaktionen stellen Datenbankzugriffe dar, die mehrere Teilschritte enthalten. Um zu gewährleisten, dass bei einem Ausfall des Systems alle Teilschritte einer Transaktion vollständig ausgeführt wurden bzw. um das System auf vollständige Transaktionen zurückzuführen, kann die Durchführung von Datenbank-Transaktionen protokolliert werden.

Dabei werden alle Änderungen an einer Datenbank in einem gesonderten Protokoll aufgezeichnet und stehen so für eine spätere Wiederherstellung zur Verfügung. Dabei ist es unerheblich, ob die Änderungen interaktiv vorgenommen oder z. B. durch einen Agenten im Batch abgearbeitet werden.



Das Register „Transaktionsprotokoll“

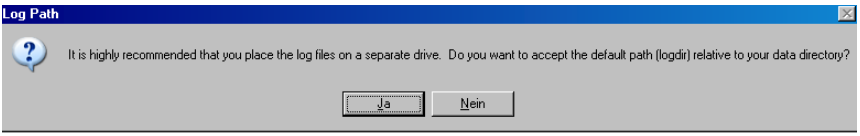
Das Transaktionsprotokoll ist mit einer Journal-Aufzeichnung vergleichbar. Bevor die Daten in die Notes-Datenbank geschrieben werden, wird zunächst die Änderung in das Transaktionsprotokoll geschrieben. Anschließend wird die eigentliche Änderung an der Datenbank durchgeführt.

Wenn eine Datenbank den Status „beschädigt“ erhält, kann mit einem Roll-Back-Verfahren wieder auf einen Stand vor der Beschädigung der Datenbank aufgesetzt werden, komplexe Wiederherstellungsmethoden können entfallen.

Im Register „Transaktionsprotokoll“ wird das Transaktionsprotokoll aktiviert, ihm wird ein Speicherplatz zugewiesen. Werden keine anderen Angaben gemacht, so wird das Transaktionsprotokoll in dem Verzeichnis „/DATA/logdir“ in der Form „Sxxxxxxxx.TXN“ abgelegt, wobei „Sxxxxxxxx“ eine eindeutige Nummer für den Domino-Server darstellt.

Wird die Transaktionsprotokollierung aktiviert, dann erscheint eine Hinweismeldung, die empfiehlt, das Transaktionsprotokoll auf einem anderen Laufwerk abzulegen, als dem, auf welchem sich das /DATA-Verzeichnis befindet.

Im Falle einer Installation von Domino auf der iSeries kann diese Meldung jedoch ignoriert werden; bei allen anderen Plattformen empfiehlt sich dieses Verfahren.



Log Path

Das Transaktionsprotokoll (engl.: Transaction Logging) wurde mit R5 eingeführt und in R6 erweitert. So steht in R6 die Protokollierung von Ansichten zur Verfügung, was im Falle einer abnormalen Systembeendigung einen wesentlichen Einfluss auf die Wiederherstellung hat, die unter Verwendung von Ansichtsprotokollierung bedeutend schneller ist. Voraussetzung für das Transaction Logging auf Ansichtsebene ist die Verwendung von ODS41 oder ODS43 (On Disk Structure).

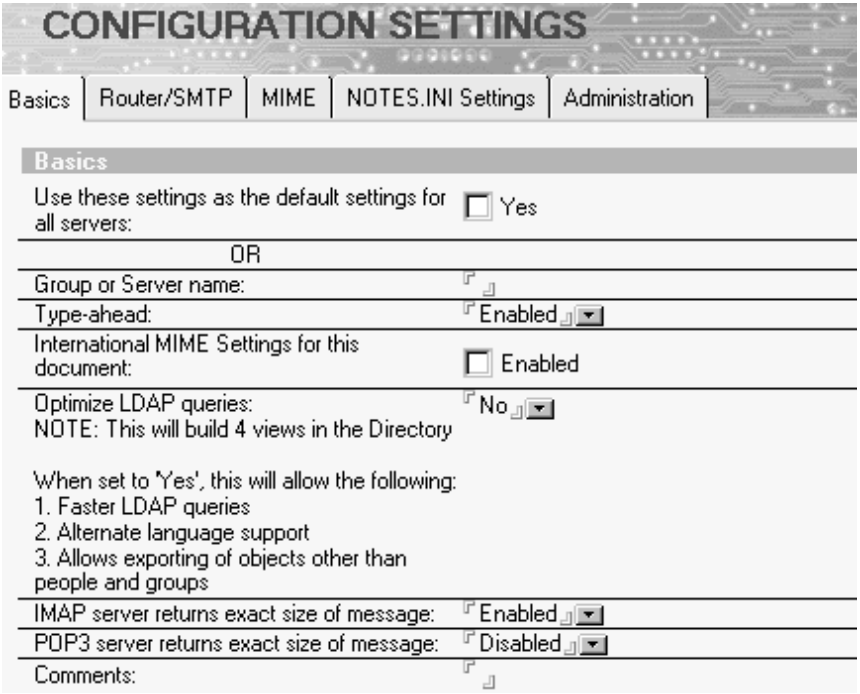
Tipp:

Im Zusammenhang mit Domino auf der iSeries kann die Datensicherung von Domino unter Verwendung von BRMS durchgeführt werden. BRMS (Backup, Recovery and Media Services) erlaubt inkrementelle Datensicherungen. Allerdings ist für diese Datensicherungsmethode das „Transaktionsprotokoll" Voraussetzung.

Diese Seite ist zur Zeit nicht belegt.

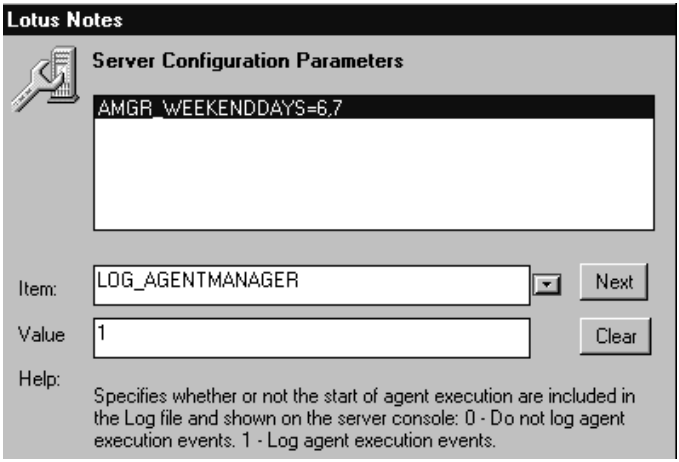
6.2 Konfigurationsdokumente

Soll das Mail-Routing für Notes- bzw. SMTP-Mails für alle oder mehrere Server einer Domäne einheitlich geregelt werden, so wird dazu ein Konfigurationsdokument verwendet.



Das Konfigurationsdokument

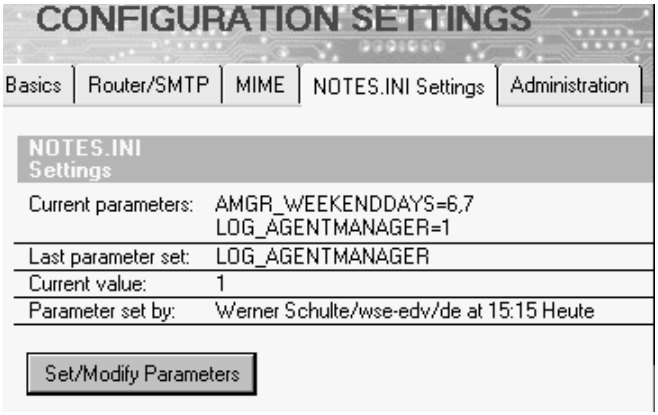
Für die notes.ini des Servers findet sich hier eine Möglichkeit, mit Hilfeunterstützung Werte einzufügen.



Parameter für die ini-Datei setzen

Die Nutzung des Dialoges ist gewöhnungsbedürftig. Sind die Felder „Item“ und „Wert“ gefüllt, werden sie mit „Weiter“ in das obere Feld übertragen. Nun kann der Parameter mit „OK“ gespeichert werden.

Die neuen Werte werden in der notes.ini des Servers gespeichert und beim nächsten Start des Servers berücksichtigt.



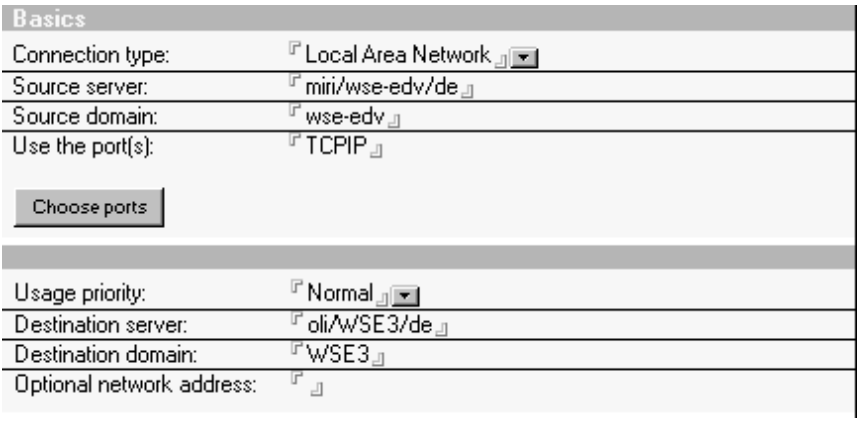
Parameter in dem Konfigurationsdokument

6.3 Verbindungsdokumente

Für die Definition des Austauschs von e-Mails und der Datenbankreplikation mit anderen Servern werden Verbindungsdokumente eingesetzt. Diese Dokumente werden immer dann benötigt, wenn sich Server in unterschiedlichen Domino-Netzwerken befinden.

6.3.1 Die LAN-Verbindung

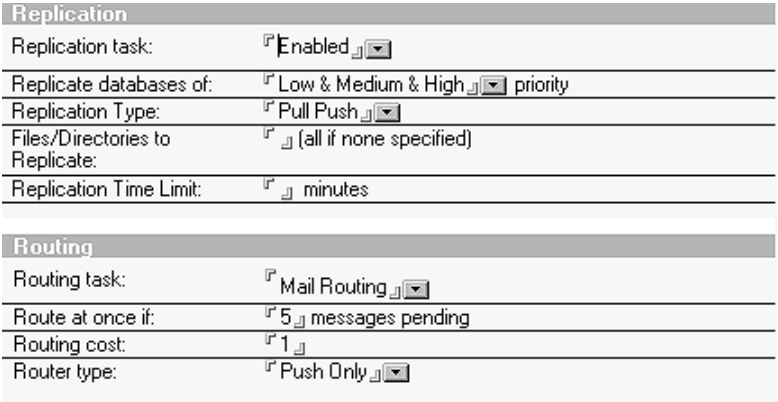
Nach Auswahl des Verbindungstyps werden der Ausgangs- und der Ziel-Server mit ihren Domänen definiert. Bei den Servern werden die vollständigen Namensangaben verwendet.



Server-Definition der Verbindung

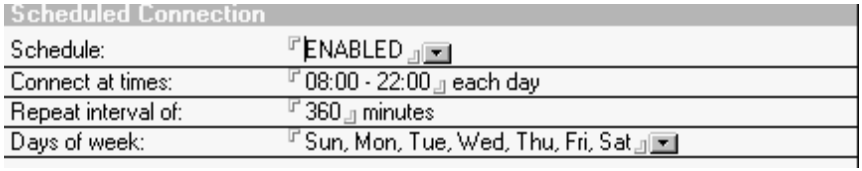
Im Register „Replikation“ wird geregelt, welche Art von Replikation zwischen den Servern stattfinden soll. Der Replikationstyp wird dazu verwendet, die Richtung der Datensynchronisation einzustellen.

Sollen nur bestimmte Datenbanken repliziert werden, können sie in ein Verzeichnis gespeichert werden, das als Replikationsverzeichnis angegeben wird.



Replikationseinstellungen

Für die Zeiteinteilung der Replikation wird das Register „Zeitplan“ verwendet. Der Zeitplan kann aktiviert oder deaktiviert werden. Ist er deaktiviert, wird keine automatische Replikation durchgeführt.

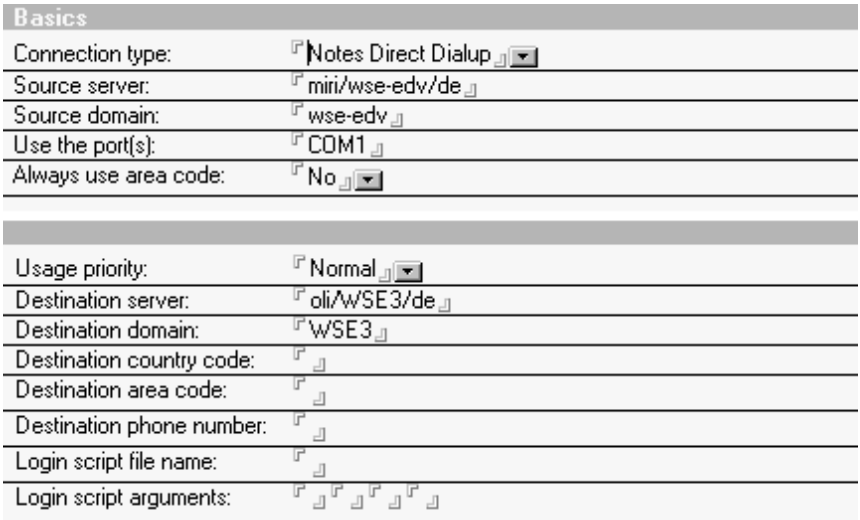


Das Register „Zeitplan“

Ist er aktiviert, können Tageszeit, Intervall und Wochentage definiert werden.

6.3.2 Notes-Direktwählverbindung

Die ursprüngliche Remote-Verbindung von Notes und Domino ist die direkte Verbindung über Modems. Dazu werden die Modem-Befehlsdateien von Domino bei der Anschluss-Definition verwendet.



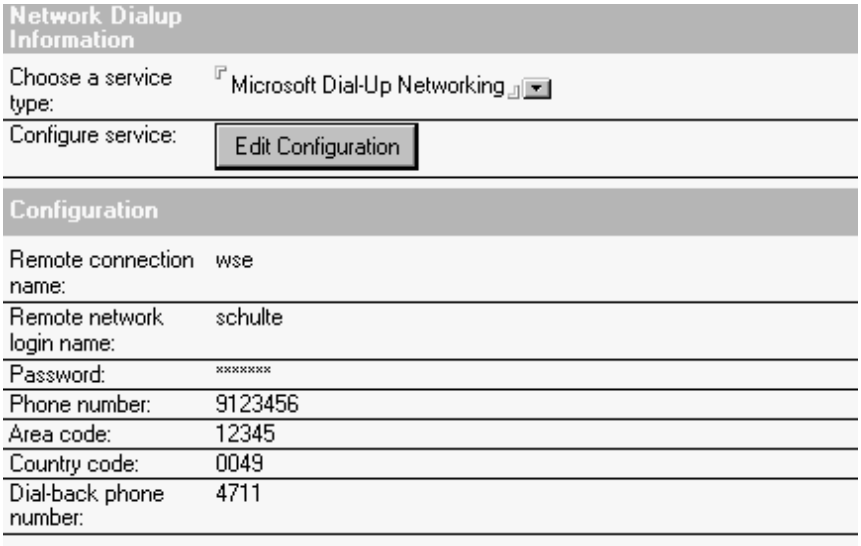
Notes-Direktverbindung

Wird als Verbindungstyp die Direktwählverbindung angegeben, erscheint im Anschlussfeld automatisch „COM1“ als Anschluss. Hängt das Modem an einem anderen Anschluss, muss das Feld angepasst werden. Außerdem können die Rufnummern und eine Script-Datei angegeben werden. Die Script-Datei wird vom Ziel-Server verwendet, um die Zugangsberechtigung zu überprüfen.

Diese Seite ist zur Zeit nicht belegt.

6.3.3 Netzwerkwählverbindung

Für die Verwendung einer RAS-Verbindung (RAS = Remote Access Service) wird die „Netzwerkwählverbindung“ ausgewählt. Das setzt natürlich voraus, dass ein RAS-Server und eine DFÜ-Verbindung vorhanden sind.



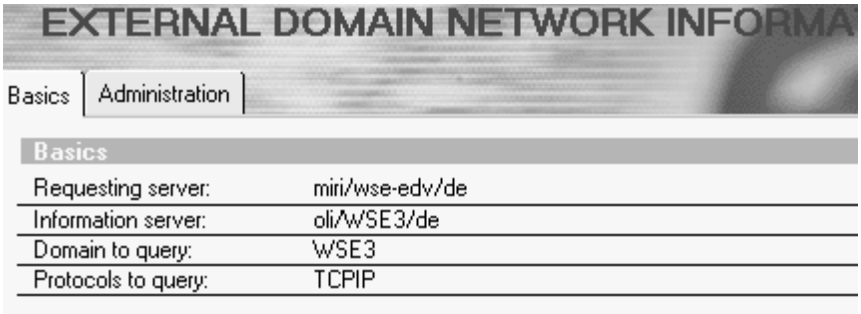
Das Register „Netzwerkwählverbindung“

Nach Auswahl dieser Anschlussart wird ein zusätzliches Register eingeblendet, in dem die Verbindungsangaben hinterlegt werden. Die Angaben werden in einer Dialogbox editiert, die über eine Schaltfläche aufgerufen wird.

Diese Seite ist zur Zeit nicht belegt.

6.4 Externe Domänen

Soll zwischen unterschiedlichen Domänen eine Kommunikation aufgebaut werden, so muss ein Dokument zur Definition der externen Domäne erstellt werden.



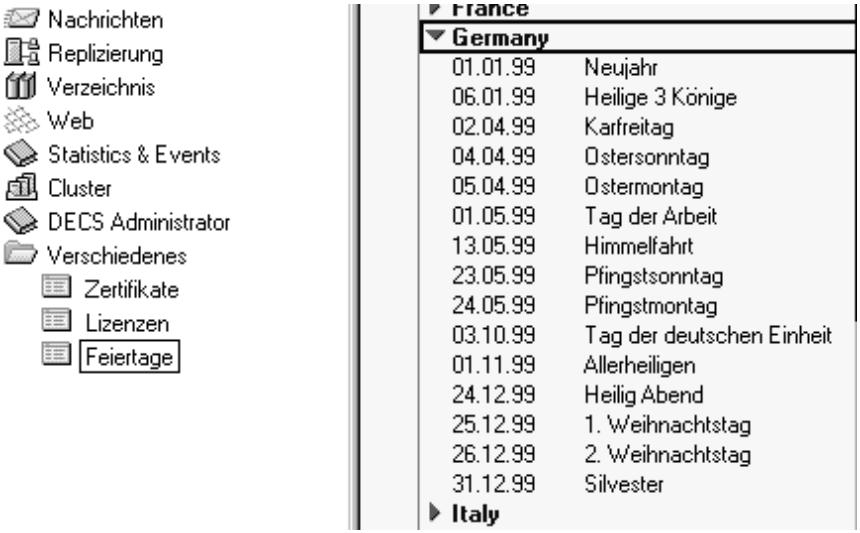
Domänendokument

Die Verbindung kann jeweils nur für ein Domino-Netzwerk definiert werden. Auf der Arbeitsstation des Clients ist nun kein Verbindungsdokument mehr zu Servern der externen Domäne erforderlich.

Diese Seite ist zur Zeit nicht belegt.

6.5 Feiertagsverwaltung

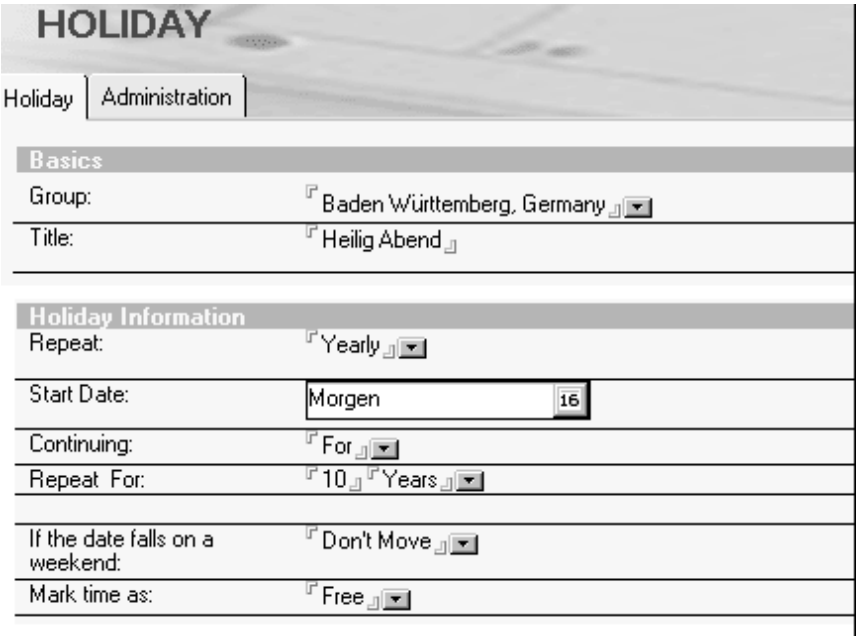
In früheren Notes- und Domino-Versionen war die Feiertagsanzeige in den Kalendern mühsame Handarbeit. Seit Release 5.0 können auf dem Server Feiertagsdokumente genutzt werden, um die benötigten Feiertage zur Verfügung zu stellen.



Standardfeiertage von Lotus

Jeder Feiertag stellt ein Dokument dar, das einzeln bearbeitet werden kann.

Soll z.B. ein Kalender für Baden-Württemberg erstellt werden, so werden die im Standardumfang enthaltenen Dokumente um das Land ergänzt.



Feiertagsdokument mit zusätzlicher Gruppe „Baden Württemberg“

Für Feiertage, die jetzt noch fehlen, oder für Betriebsferien, werden neue Dokumente erstellt, die nur die neue Gruppe enthalten. Damit ist der Administratorteil der Feiertagsverwaltung erledigt.

Der Benutzer kann jetzt in seinem Kalender unter „Werkzeuge / Feiertage einfügen“ die Feiertage für Baden Württemberg übernehmen.

Feiertage im Kalender einfügen

Da einzelne Feiertage nicht immer auf den gleichen Kalendertag fallen, müssen die Kalenderdokumente auf dem Server jährlich überarbeitet werden.

Diese Seite ist zur Zeit nicht belegt.

6.6 Verzeichnisse in Lotus Domino

Zur Adresssuche und Adresszuordnung in E-Mail-Dokumenten greifen Lotus Domino und Notes auf Verzeichnisse zu, die Adressinformationen enthalten. Die Adressinformationen werden in zwei Situationen gesucht:

- bei der Schnelladressierung

  Jedes Mal, wenn ein Zeichen in ein E-Mail-Empfängerfeld eingegeben wird, versucht der Notes-Client den Rest der Adresse automatisch zu ergänzen. Dazu sucht er in Verzeichnissen.

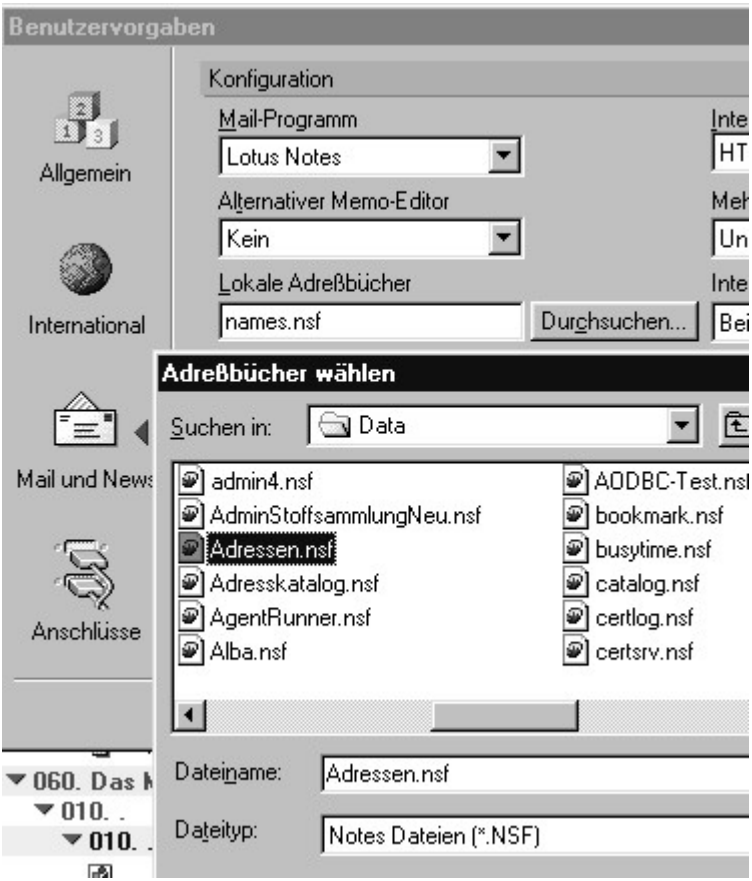
- bei der endgültigen Adressauflösung

  Sobald der Benutzer eine Aktualisierung auslöst, wenn das Dokument gespeichert oder versendet wird, setzt der Notes-Client die endgültige Adresse des Empfängers in das „SendTo"-Feld ein. Dazu durchsucht er alle bekannten Verzeichnisse.

Als Basis dienen dazu die Adressbücher aus Lotus Domino, das persönliche Adressbuch des Benutzers und das Domino-Verzeichnis (das öffentliche Adressbuch) der Domäne. Neben diesen Standardverzeichnissen können noch weitere Verzeichnisse genutzt werden:

- Eigene Adressdatenbanken, die mit der Schablone „PUBNAMES.NTF" erstellt wurden
- Domino-Verzeichnisse anderer Domänen
- LDAP-Verzeichnisse anderer Systeme
- Verzeichniskataloge
- Verzeichnisse, die in der Domino-Verzeichnisverwaltung hinterlegt sind

Eine spezielle Such-Unterstützung bieten die kaskadierenden Adressbücher. Bei diesem Verfahren werden Adressdatenbanken in der Datei „Notes.ini“ mit dem Eintrag „NAMES“ hinterlegt. Die Adressdatenbanken können auch im Notes-Client über das Menü „Datei / Vorgaben / Benutzervorgaben / Mail und News“ eingetragen werden.



Kaskadierende Adressbücher eintragen

Der Client durchsucht die Datenbanken dann in der Reihenfolge, in der sie in der „Notes.ini“ aufeinander folgen. Dieses Verfahren ist das älteste und kann auch in R5 noch verwendet werden. Lotus weist darauf hin, dass dieses Verfahren nicht weiter ausgebaut und auf längere Zeit gesehen auch nicht mehr unterstützt wird.

Mit der Änderung des Namens von „Öffentliches Adressbuch“ in „Domino-Verzeichnis“ wendet sich Lotus hin zur allgemeinen Integration von Domino in die Welt des Internets. Der Domino-Server kann jetzt auch als Server für E-Mail-Systeme eingesetzt werden, die über das LDAP-Protokoll nach Adressinformationen suchen. Auch umgekehrt kann Lotus Domino Adressinformationen aus fremden LDAP-Servern abrufen.

Zur Unterstützung dieser Dienste wurden verschiedene Datenbanken und Server-Prozesse eingeführt. Als LDAP-Dienst kann ein Prozess mit dem Namen „LDAP“ gestartet werden. Dieser Prozess kann bei der Konfiguration des Domino-Verzeichnisses oder auch später durch eine Anpassung installiert werden. Er wird durch einen entsprechenden Tasks-Eintrag in der „Notes.ini“ gestartet.

Diese Seite ist zur Zeit nicht belegt.

6.6.1 Der Verzeichnis-Katalog

Bei größeren Unternehmen kann das Domino-Verzeichnis einen erheblichen Umfang annehmen. In diesem Fall ist die Verteilung dieser Daten im Wege der Replikation zeitraubend und aufwendig. Deshalb wurde eine neue Datenbank und ein dazugehöriger Prozess eingeführt, um die Adressdaten zu extrahieren und auf den notwendigen Umfang zu reduzieren. Über den Directory-Cataloger-Prozess werden die Adressinformationen aus verschiedenen Verzeichnissen abgeglichen und bestimmte Felder in die Katalogdatenbank übernommen. Für unterschiedliche Zwecke können unterschiedliche Katalogdatenbanken angelegt werden. Durch diese Vorgehensweise wird erreicht, dass die Größe einer solchen Datenbank wesentlich kleiner ist als ein normales Domino-Verzeichnis. Das ist natürlich besonders vorteilhaft, wenn mobile Clients eingesetzt werden. Damit ein Verzeichniskatalog für einen mobilen Client erstellt werden kann, muss zunächst ein solcher auf einem Server erstellt werden. Der Server kann der gleiche sein, der auch die Mail-Server-Funktion wahrnimmt. Es kann aber auch ein spezieller Verzeichnis-Server eingerichtet werden.

Februar 2001 / 4. EL

6.6.1.1 Die Installation des Verzeichniskataloges

Unabhängig davon, ob ein Verzeichniskatalog nur auf einem Server oder auf mehreren Servern verwendet werden soll, wird der dircat-Prozess nur auf einem Server installiert, um Replikations-Probleme auszuschließen.

❶❷❸ Ausführungsschritte:

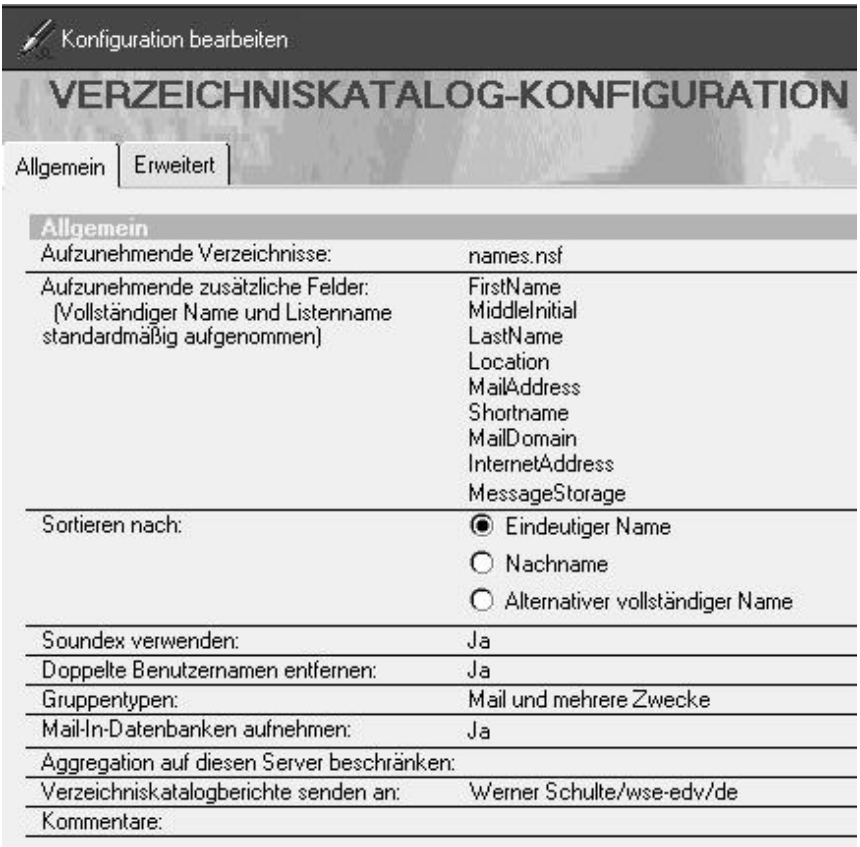
- Verzeichnisse, die verwendet werden sollen, auf den Server des Verzeichniskataloges replizieren
- Verzeichniskatalog erstellen
- Konfigurationsdokumente erstellen
- Repliken auf Servern und Arbeitsstationen erstellen

❶❷❸

Ist der Server ausgewählt, auf dem der Verzeichniskatalog seine Arbeit tun soll, so sollten dort zunächst Repliken aller Verzeichnisse erstellt werden, die der Verzeichniskatalog verwenden wird. Damit wird die Arbeit des dircat-Prozesses wesentlich beschleunigt. Dann kann der Katalog selbst über den Datenbank-Neu-Dialog aus der Schablone „dircat5.ntf“ angelegt werden. Die neue Datenbank enthält nur zwei Ansichten:

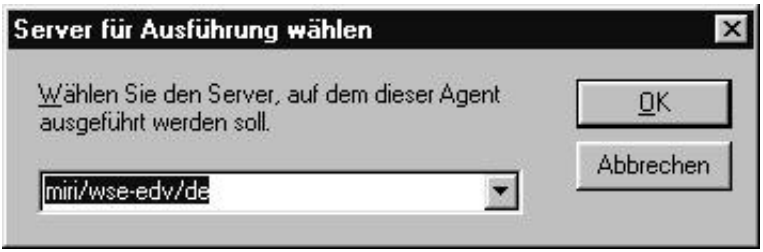
- Benutzer
- Konfigurationen

Über das Menü „Erstellen“ wird ein Dokument „Konfiguration“ erstellt. In diesem Dokument wird definiert, welche Datenbanken in dem neuen Katalog zusammengefasst werden sollen.



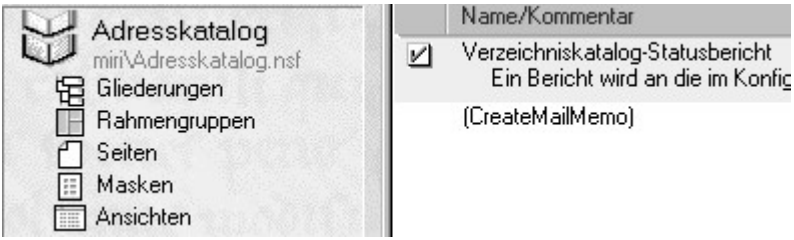
Konfiguration des Verzeichniskataloges

Standardmäßig werden die Felder angegeben, die für die Aufgaben der Adressfindung benötigt werden. Weitere Felder können zwar angegeben werden, sollten aber sehr sorgfältig ausgewählt werden, da damit der Umfang des Kataloges wächst. Das widerspricht aber dem Ziel, ein möglichst kleines Adressverzeichnis zu erzielen. Zur besseren Überwachung der Funktion des Verzeichniskataloges kann noch angegeben werden, wer eine E-Mail mit Berichten über Aktivitäten des dircat-Prozesses erhalten soll. Beim Speichern der Konfiguration wird gefragt, auf welchem Server der Agent laufen soll, der die Berichte erzeugt.



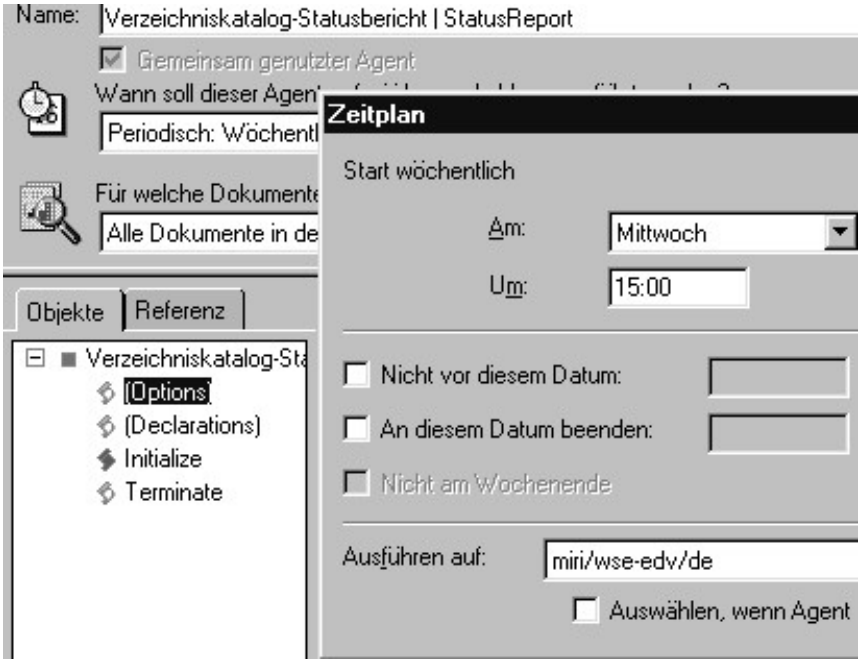
Serverabfrage

Dieser Agent läuft sonntags um 2:00 Uhr morgens. Falls das nicht gewünscht wird, sollte diese Einstellung geändert werden.



Agent für den Statusbericht

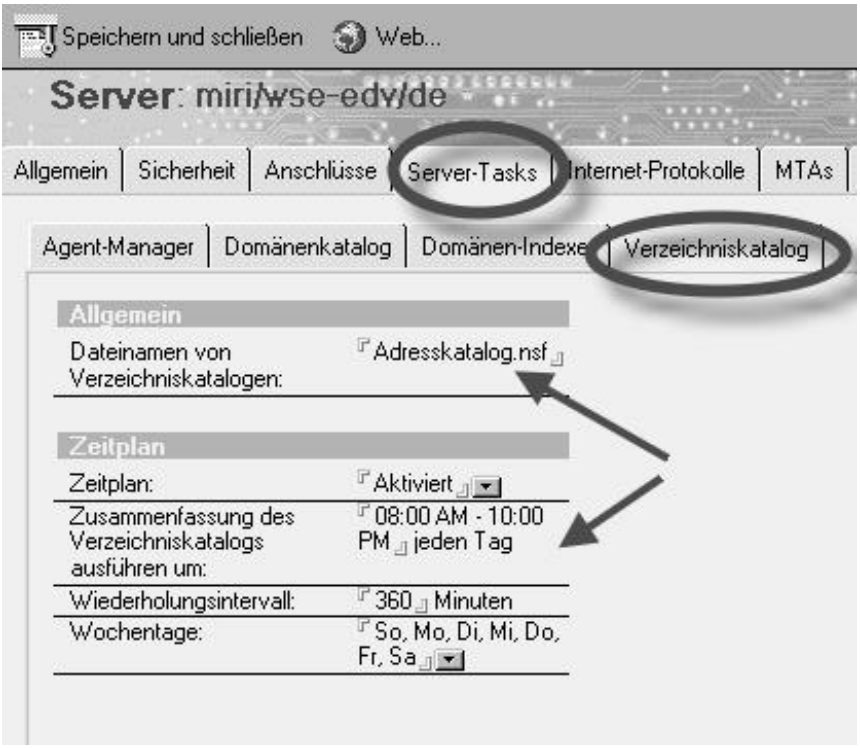
Vor allem, wenn der Server nicht ständig aktiv ist, sollte eine Zeit gewählt werden, zu welcher der Server normalerweise läuft.



Zeitplan ändern

Damit ist die Konfiguration abgeschlossen und die Benutzer können in dem Katalog angelegt werden. Damit das geschieht, muss der dircat-Prozess gestartet werden. Der Prozess geht durch alle angegebenen Verzeichnisdatenbanken und erstellt für jeden Benutzer, jeden Server, jede Gruppe und Ressource ein Dokument mit der Kontakt-Maske und füllt die in der Konfiguration genannten Felder.

Der dircat-Prozess wird über einen Eintrag im Serverdokument gestartet.



Eintrag im Serverdokument

Dazu kann über den Administrator-Client im Konfigurationsregister das aktuelle Serverdokument geöffnet und im Abschnitt „Server-Tasks“ das Register „Verzeichniskatalog“ angewählt werden. Hier werden die Namen der Verzeichniskatalog-Datenbanken eingetragen. Außerdem wird der Zeitplan aktiviert und kann nach Bedarf geändert werden.

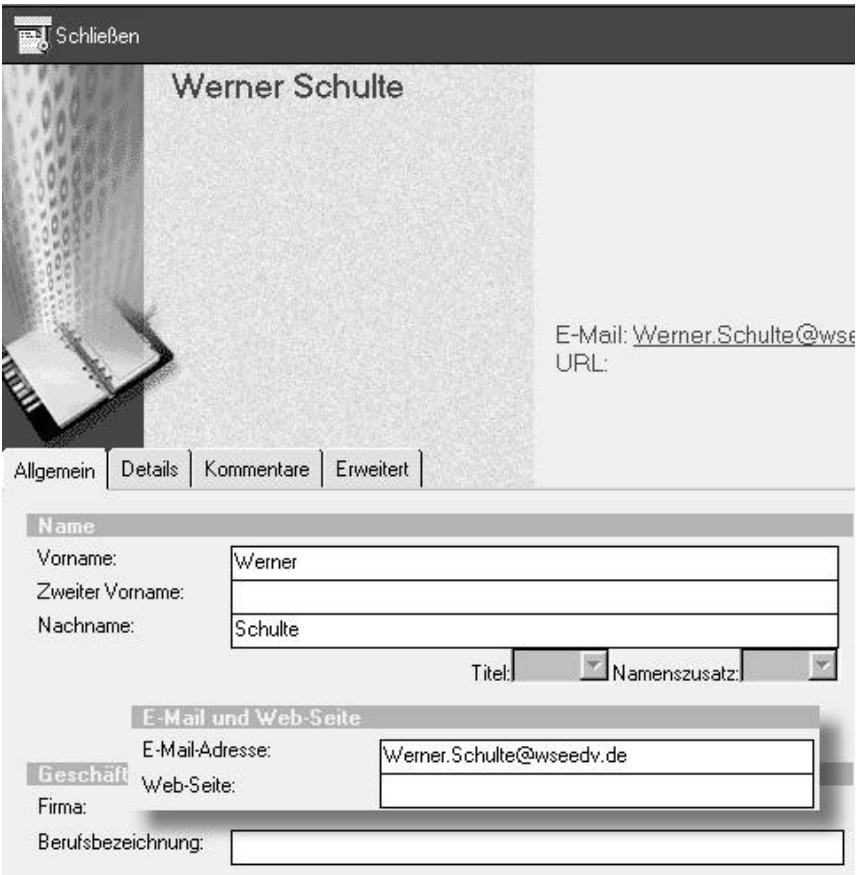
❶❷❸ Ausführungsschritte:

1. Administrator-Client starten
2. Bereich „Konfiguration“ anwählen
3. In der Gliederung auf der linken Seite Server und aktuelles Serverdokument auswählen
4. Im Serverdokument das Register „Server-Tasks“ anklicken
5. Den Abschnitt „Verzeichniskatalog“ auswählen
6. Die Verzeichniskataloge eintragen und den Zeitplan bearbeiten

❶❷❸

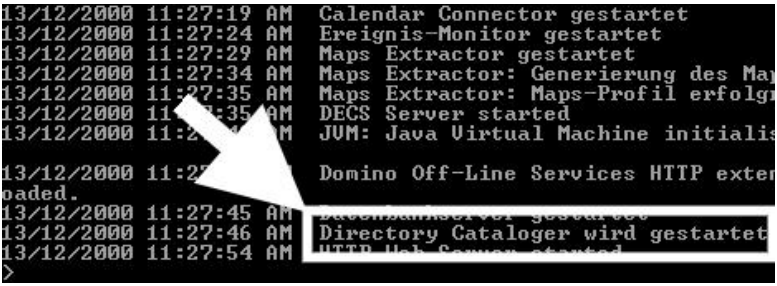
Der dircat-Prozess kann auch manuell gestartet werden. Das geht allerdings nur, wenn er nicht gerade aktiv ist. Der manuelle Start kann, wie bei jedem Prozess über die Konsole (load dircat Adresskatalog.nsf) oder über den Administrator-Client erfolgen. Beim ersten Start erstellt der Prozess die Namensdokumente. Später werden sie an Änderungen angepasst.

Wird das Konfigurationsdokument geändert, werden alle Benutzer-Dokumente neu erstellt. Das Erstellen aller Dokumente eines Verzeichniskataloges kann, je nach Anzahl der Personendokumente, sehr lange dauern.



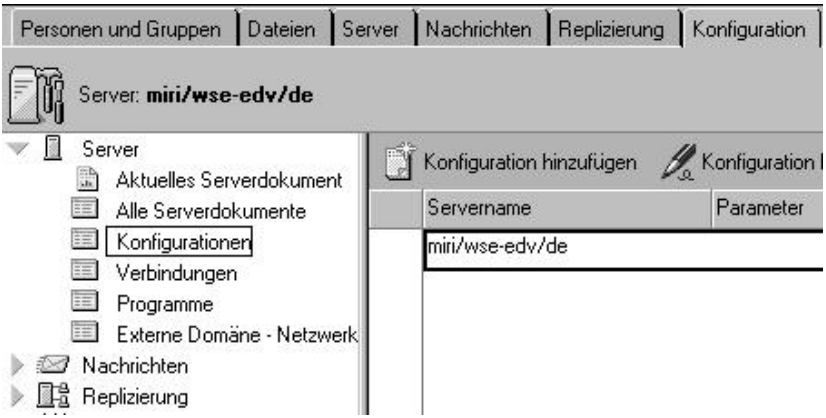
Benutzerdokument im Verzeichniskatalog

Ist der Prozess im Serverdokument eingetragen, wird er beim Start des Servers zusammen mit den anderen Server-Prozessen aktiviert.



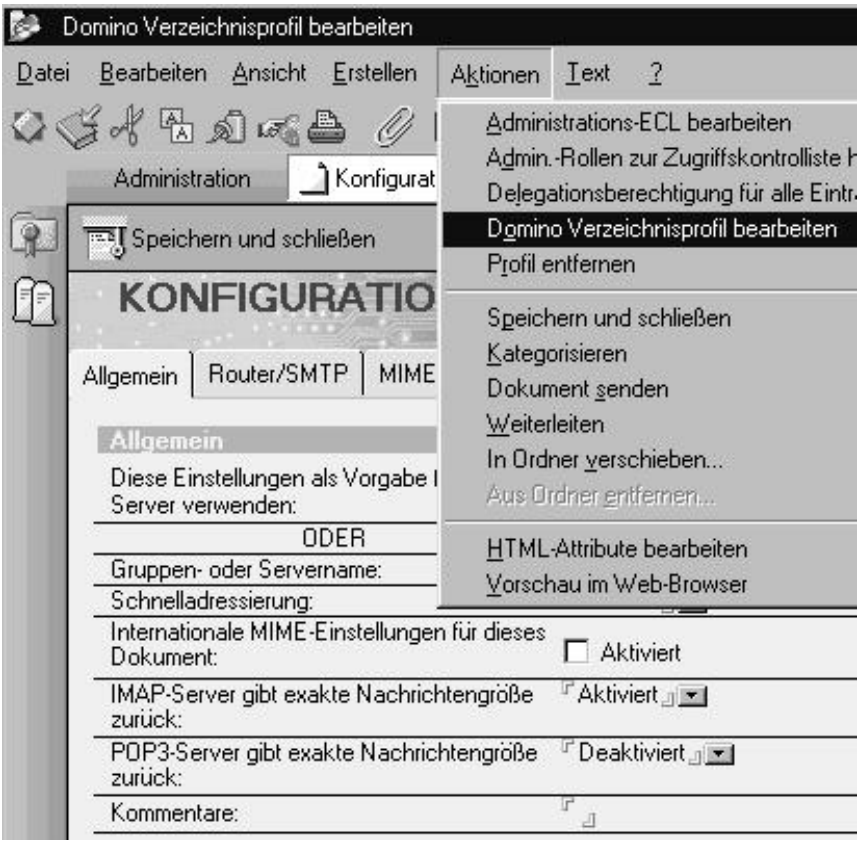
Start des dircat-Prozesses

Zum Abschluss der Server-Installation muss noch das Verzeichnisprofil des Domino-Verzeichnisses einen Eintrag für den Verzeichniskatalog erhalten. Dazu wird über den Administrator-Client unter den Server-Einträgen die Position „Konfigurationen“ ausgewählt und das Profil-Dokument des Servers geöffnet.



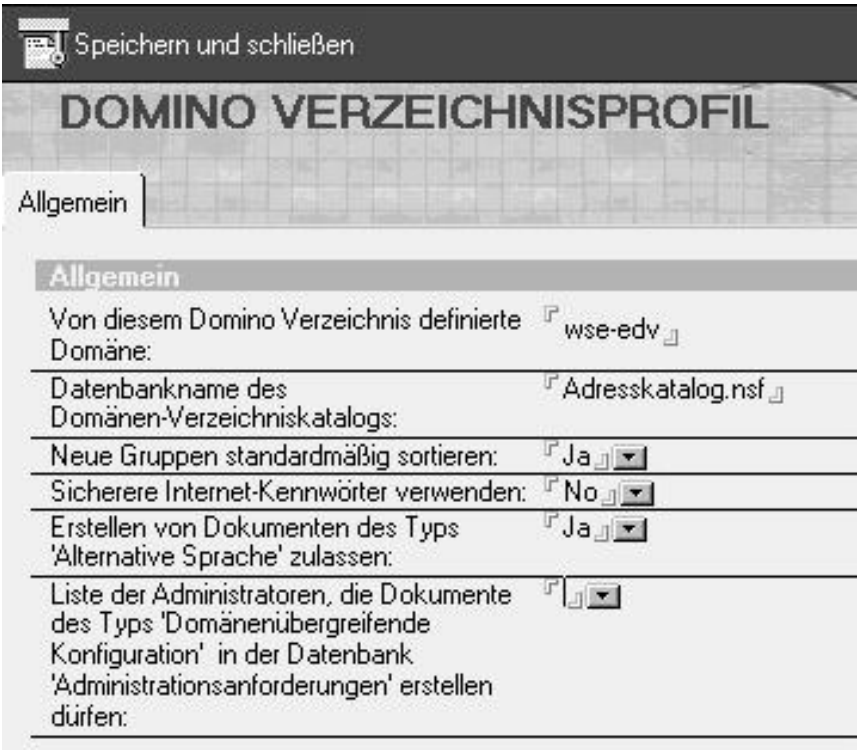
Konfigurationsprofile

Im Menü „Aktionen“ findet sich die Position „Dominoverzeichnis bearbeiten“.



Domino-Verzeichnisprofil bearbeiten

Hiermit wird ein Dialog zum Bearbeiten des Verzeichniskatalogeintrages geöffnet.



Domino-Verzeichnisprofil

Unter „Datenbankname des Domänen-Verzeichniskatalogs“ wird der Verzeichniskatalog eingetragen. Sollen Gruppen bei deren Übernahme alphabetisch sortiert werden, so kann das hier ebenfalls gesteuert werden.

6.6.1.2 Der Verzeichniskatalog auf den Arbeitsstationen

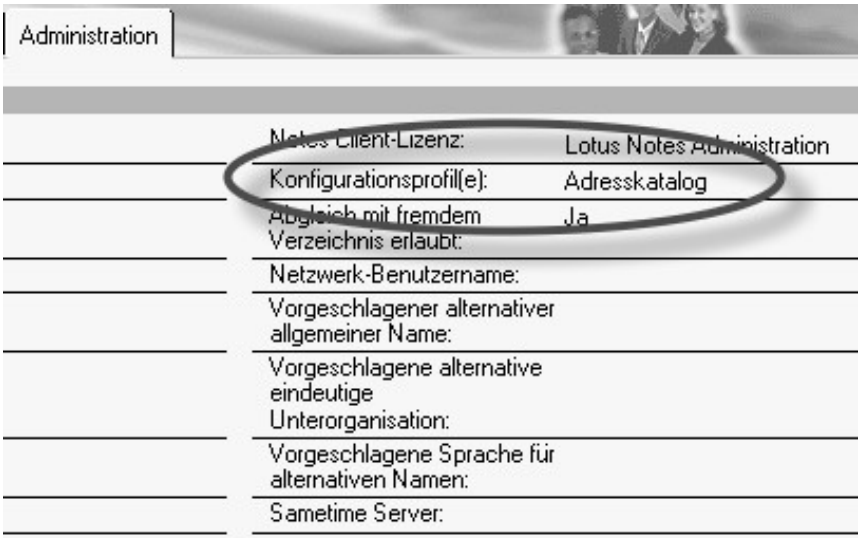
Ist die Installation und Konfiguration des Verzeichniskataloges auf dem Erstellungsserver abgeschlossen, kann er auf andere Server, die ihn verwenden sollen, repliziert werden. Außerdem steht er jetzt auch zum Einsatz auf den Arbeitsstationen zur Verfügung. Um die Katalogdatenbank auf alle Arbeitsstationen zu verteilen, müssen folgende Schritte ausgeführt werden:

- Replikation des Verzeichniskataloges für jede Arbeitsstation erstellen
- in der Datei „Notes.ini“ unter dem Eintrag „NAMES“ die Katalogdatenbank eintragen

  oder:

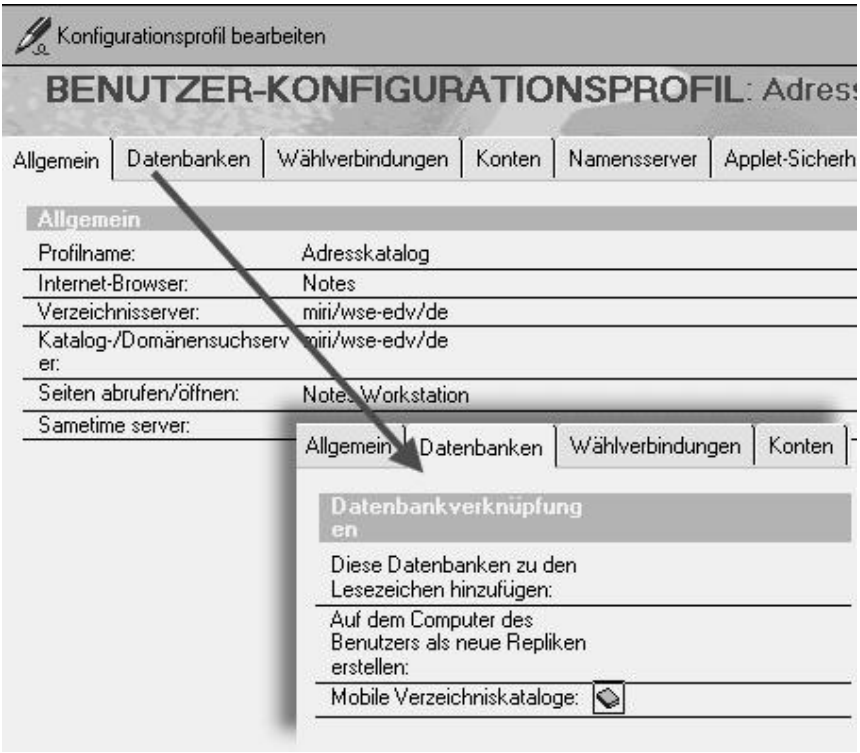
- über die Benutzervorgaben den Eintrag in der Datei „Notes.ini“ erstellen

Diese Aufgabe kann auch automatisch erledigt werden, wenn mit Benutzerkonfigurationsprofilen gearbeitet wird. Dazu muss bei den betroffenen Benutzern der Name des Konfigurationsprofils im Personendokument des Domino-Verzeichnisses eingetragen sein.



Benutzer-Konfigurationsprofil im Personendokument

In diesem Konfigurationsprofil wird jetzt eine Datenbankverknüpfung mit dem Verzeichniskatalog eingefügt. Dazu wird der Verzeichniskatalog auf dem Server geöffnet und über das Menü „Bearbeiten / Als Verknüpfung kopieren / Datenbankverknüpfung“ ein Link zu der Datenbank in die Zwischenablage kopiert. Dann wird das Konfigurationsprofil geöffnet.



Datenbankverknüpfung im Konfigurationsprofil

Im Abschnitt „Datenbanken“ unter „Datenbankverknüpfungen“ befindet sich das Feld „Mobile Verzeichniskataloge“, in das die Verknüpfung mit der Menüposition „Bearbeiten / Einfügen“ gespeichert wird. Dieser Eintrag sorgt bei der nächsten Serververbindung der Benutzer mit diesem Konfigurationsprofil dafür, dass der Verzeichniskatalog automatisch in das Arbeitsverzeichnis dieser Benutzer repliziert wird.

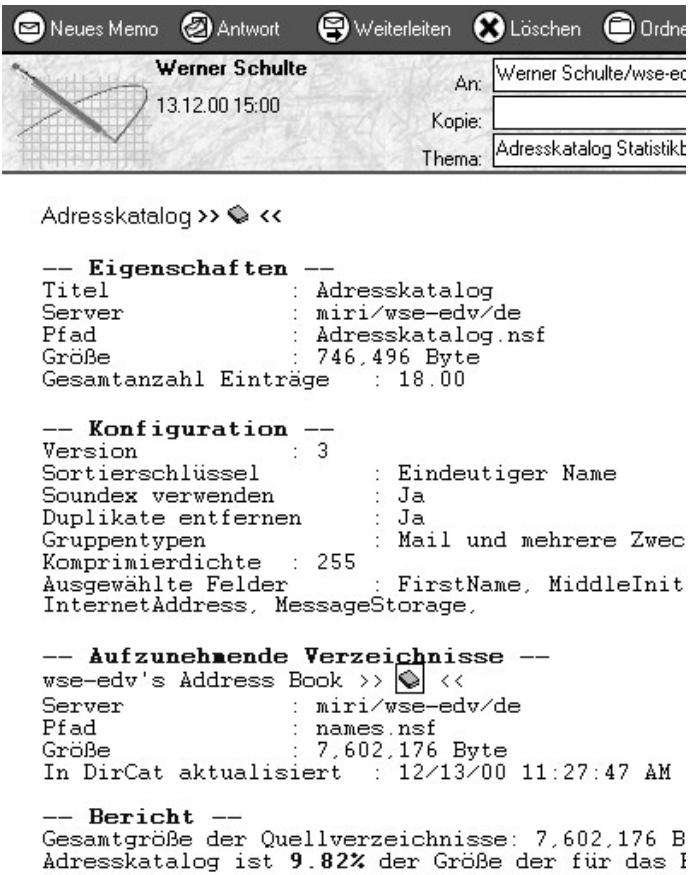
```
WinNTIconHidden=0
WinNTIconRect=0 0 1024 24
FileDlgDirectory=J:\Lotus\Domino\Data
Praxis\Bilder
PhoneLog=2
Log=log.nsf, 1, 0, 7, 40000
NewMailSeqNum=1316
NewMailSeqNumC1256808:0047A578=1316
BCASEWINDOWSIZE=-4 -4 1032 748
NAMES=names.nsf,Adresskatalog
$headlineDisableHeadlines=0
```

Eintrag des Verzeichniskataloges in der „Notes.ini“

Auch der Eintrag in die Datei „Notes.ini“ wird damit erledigt. Diese Aufgabe übernimmt das Programm „ndycfg.exe“ (Notes Dynamic Configuration) auf der Arbeitsstation.

6.6.1.3 Überwachung des Verzeichniskatalogs

Auf zwei unterschiedlichen Wegen kann die Überwachung des dircat-Prozesses erfolgen. Der eine Weg besteht darin, den Empfänger des Änderungsberichtes im Konfigurationsdokument des Verzeichniskataloges einzutragen.



Bericht über eine Änderung des Verzeichniskataloges

Dieser Benutzer wird über eine E-Mail informiert, wenn eine Änderung erfolgt. Die E-Mail ist als Bericht aufgebaut, der Angaben zu Größe, Anzahl der Einträge und den Umfang der Platzersparnis enthält. Die zweite Möglichkeit, Informationen zu erhalten, besteht in der gewohnten Methode des Eintrages in der Datei „Notes.ini“. Der Eintrag

```
Log_DirCat=1
```

bewirkt, dass in der Log-Datenbank ein Eintrag mit Startzeit, Endzeit und Name des Verzeichniskataloges erstellt wird.

Diese Seite ist zur Zeit nicht belegt.

6.6.2 Verzeichnisverwaltung

Als neueres Verfahren zur Zusammenführung von Adressen im Verhältnis zu den kaskadierenden Adressbüchern verwendet Lotus Domino die Verzeichnisverwaltung. Bei diesem Verfahren werden wie bei dem Verzeichniskatalog die Adressinformationen verschiedener Adressbücher zu einem gemeinsamen Verzeichnis zusammengefasst. Der Bedarf an einer solchen Zusammenfassung entsteht dann, wenn in einem Unternehmen verschiedene Domänen mit unterschiedlichen Adressbüchern oder Adressverzeichnisse anderer Systeme eingesetzt werden. Spezielle Adressbücher können auch dadurch entstehen, dass z. B. Kunden- oder Lieferantenadressen in einer Domino-Adressdatenbank außerhalb des Domino-Verzeichnisses verwaltet werden. Zur Einrichtung von Verzeichnisverwaltungen bietet das Domino-System die Datenbankschablone DA50.NTF an. Es wird eine neue Datenbank erstellt, die von dieser Schablone abhängt, deren Name jedoch frei vergeben werden kann. In der neuen Datenbank werden Dokumente erstellt, die definieren, welche Verzeichnisse zusammengefasst werden sollen. Lotus spricht in diesem Zusammenhang von einem „Sekundären Domino-Verzeichnis“, da es sich nicht um das Domino-Verzeichnis einer Domäne handelt. Die Funktionen der Verzeichnisverwaltung sind:

- Zugriffe aus dem Internet überprüfen, wenn der Domino-Server als Web-Server eingesetzt wird.
- Die Namens- und Adress-Suche auf Domino und LDAP-Verzeichnisse erweitern, die in der Verzeichnis-Verwaltungsdatenbank aufgeführt sind.

Mai 2001 / 5. EL

6.6.2.1 Verzeichnisverwaltung einrichten

Über das Menü „Datei / Datenbank / Neu“ wird eine neue Verzeichnis-Verwaltungsdatenbank mit beliebigem Namen angelegt. Als Schablone wird Verzeichnisverwaltung (DA50.NSF) verwendet. Auf jedem Server, der mit der Verzeichnisverwaltung arbeiten soll, wird eine Replik der Datenbank erstellt.

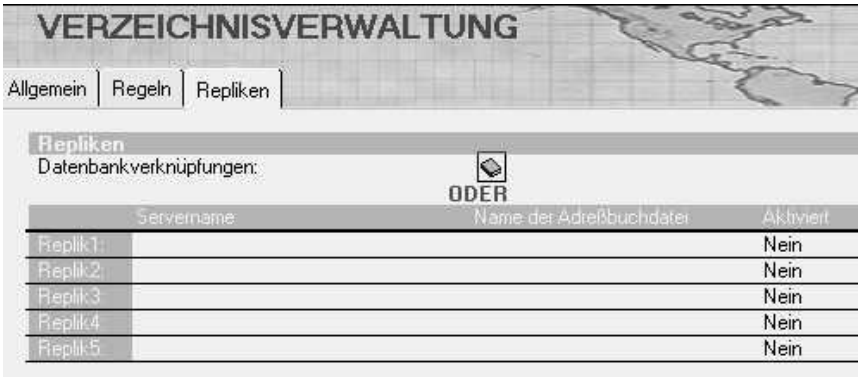
Durch „Verzeichnisverwaltung hinzufügen“ muss ein Konfigurationsdokument für jedes einzubindende Verzeichnis in der neuen Datenbank erstellt werden. Für Notes-Verzeichnisse muss der Domänentyp „NOTES“ gewählt werden. Für sekundäre Verzeichnisse muss ein vom Notes-Domänenname abweichender beliebiger Name im Feld „Domänenname“ vergeben werden. Das ist entweder der Name der Domäne dieses Verzeichnisses oder ein frei gewählter Name. Der Name der aktuellen Domäne darf hier nicht verwendet werden. Im Feld „Aktiviert“ ist „Ja“ einzutragen, um das Verzeichnis nutzen zu können.

Verzeichnis definieren

Um ein Verzeichnis einzubinden, wird eine Replik dieses Verzeichnisses geöffnet und über das Menü „Bearbeiten / Als Verknüpfung kopieren / Datenbankverknüpfung“ ein Datenbank-Link in die Zwischenablage von Windows gestellt.

Danach wird in das neue Konfigurationsdokument zurückgewechselt, und im Abschnitt „Repliken“ wird im Feld Datenbankverknüpfungen mit „Bearbeiten / Einfügen“ der Datenbank-Link auf das einzubindende Verzeichnis aus der Windows-Zwischenablage wieder eingefügt.

Verknüpfungen können nur dann verwendet werden, wenn es sich um Server ab Release 5 handelt und die Server ständig verfügbar sind.

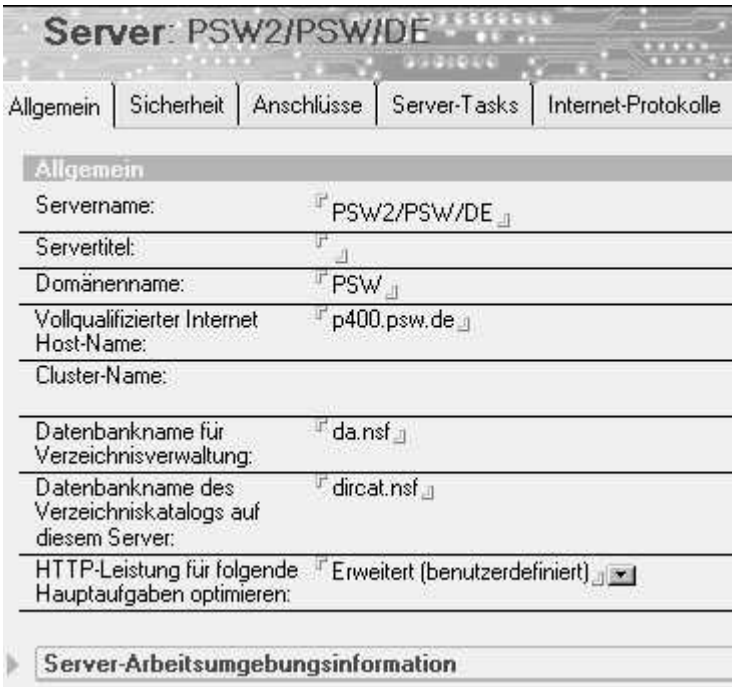


Datenbankverknüpfung einfügen

Soll ein LDAP-Verzeichnis eingesetzt werden, um Benutzer eines anderen Systems bei der Adressierung von e-Mails oder zur Authentifizierung von Web-Clients finden zu können, so wird als

Domänentyp „LDAP“ eingesetzt. Im Register „LDAP“ sind dann die Angaben zu dem Host zu machen, auf dem sich das Verzeichnis befindet.

Im Server-Dokument jedes Servers, der die Datenbank für die Verzeichnisverwaltung verwenden soll, wird im Register „Allgemein“ im Feld „Datenbankname für Verzeichnisverwaltung“ der Dateiname der erstellten Verzeichnis-Verwaltungsdatenbank eingetragen.



Verzeichnisverwaltung im Server-Dokument

Gruppen eines LDAP-Verzeichnisses, das in der Verzeichnisverwaltung aufgeführt ist, können in den Zugriffskontroll-Listen von Datenbanken eingesetzt werden.

Diese Seite ist zur Zeit nicht belegt.

6.6.3 Vergleich der Verzeichnissysteme

Die Verzeichnissysteme „Verzeichniskatalog“, „Kaskadierende Adressbücher“ und „Verzeichnisverwaltung“ haben teilweise die gleichen, teilweise aber auch unterschiedliche Funktionen. Deshalb hier eine kurze Übersicht über die Einsatzmöglichkeiten der Systeme:

	Mobiler Verz. Katalog	Server Verz. Katalog	Verz. Verwaltg.	Kaskad. Adress-bücher
Adress-Suche in sekundären Domino-Verzeichnissen für Notes-Benutzer	Ja	Ja	Ja	Ja
Schnelladressierung	Ja	Ja	Ja	Ja
Adress-Suche in LDAP-Verzeichnissen für Notes-Benutzer	Nein	Nein	Ja	Nein
Adress-Suche in sekundären Domino-Verzeichnissen für LDAP-Clients	Nein	Ja	Ja	Ja
Web-Clients über Einträge in sekundären Domino-Verzeichnissen authentifizieren	Nein	Ja	Ja	Nein

Kurzgefasst kann gesagt werden:

- Kaskadierende Adressbücher sollten durch die Verzeichnisverwaltung ersetzt werden.
- Die Verzeichnisverwaltung unterstützt LDAP-Funktionen wesentlich umfangreicher als der Verzeichniskatalog.

- Der Verzeichniskatalog erlaubt es, sehr viele Adressen unter Verwendung von relativ wenig Speicherplatz zu verwalten.

Sind mehrere Verzeichnissysteme installiert, werden sie in folgender Reihenfolge durchsucht:

- **Domino-Server**
  1. Das Domino-Verzeichnis der Domäne
  2. Die in der Datei „Notes.ini“ unter dem Eintrag „Names“ aufgeführten Adressbücher oder Verzeichnisse. Handelt es sich um kaskadierende Adressbücher endet die Suche hier.
  3. Der Verzeichniskatalog (wenn er installiert wurde).
  4. Die Verzeichnisverwaltung
- **Notes-Clients**
  1. Das persönliche Adressbuch (NAMES.NSF)
  2. Der Mobile Verzeichniskatalog (falls ein solcher vorhanden ist).
  3. Weitere Suche auf dem Server (je nach Einstellungen in der aktuellen Arbeitsumgebung).

7

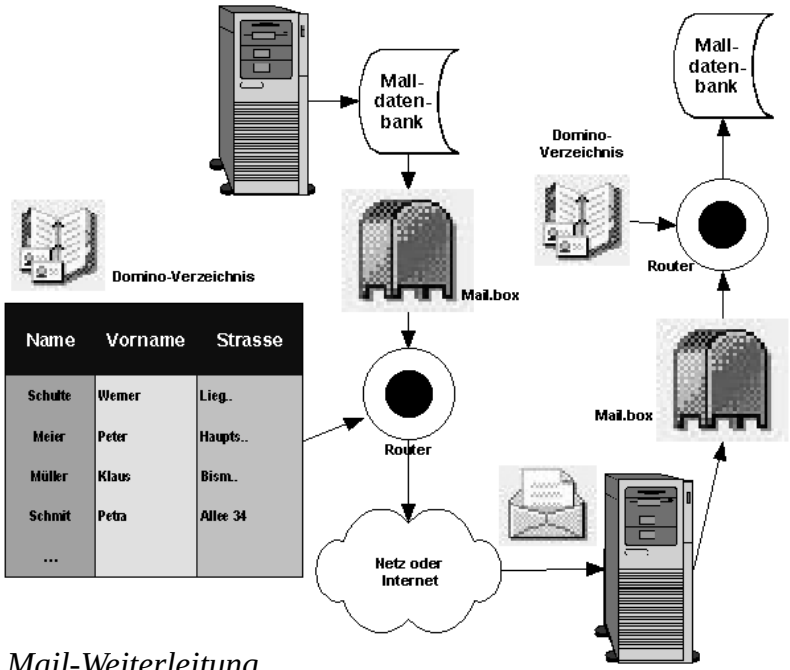
Die Verwaltung des e-Mail-Systems

Bei der Anlage eines neuen Benutzers wird von Lotus Domino im „Mail“-Verzeichnis des Servers automatisch eine Mail-Datenbank für diesen Benutzer angelegt. Die Mail-Datenbank enthält sowohl Daten (eingehende und ausgehende e-Mails, Kalenderdokumente und Aufgabendokumente) als auch die Programme, die für die Verwendung der Daten erforderlich sind.

Die Weiterleitung der e-Mails erledigt ein spezieller Prozess des Servers, der Router. Er übernimmt e-Mails aus der Datenbank „Mail.box“, die ein Benutzer erstellt hat, und liefert sie an den Server oder die Mail-Datenbank des Empfängers aus. Eingehende e-Mails liefert der Router-Prozess an die Mail-Datenbank des Benutzers aus, der als Empfänger in der Nachricht eingetragen ist.

Zwei Elemente verwendet der Router-Prozess bei seiner Arbeit:

- die Datenbank Mail.box als Zwischenlager für gesendete, aber noch nicht weitergeleitete e-Mails
- das Domino-Verzeichnis der Domäne (names.nsf) zur Ermittlung der genauen Empfänger-Adresse

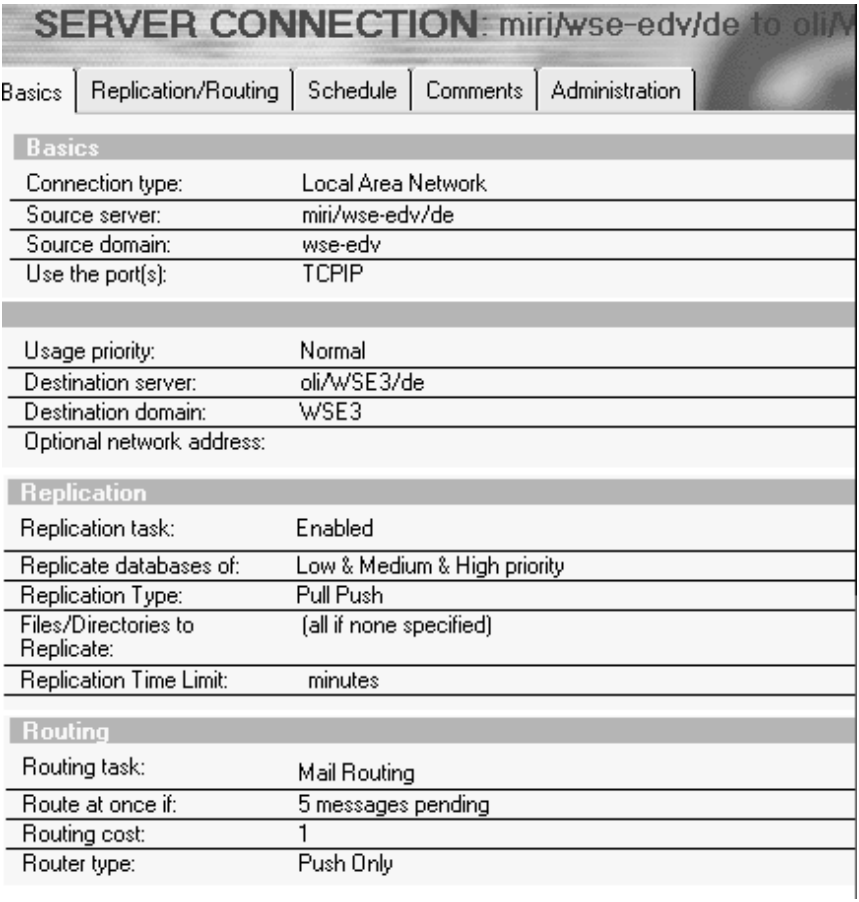


Mail-Weiterleitung

7.1 Server-Verbindungen

Innerhalb eines Domino-Netzwerkes werden Nachrichten ohne spezielle Verbindungsdokumente ausgeliefert. Befindet sich die Mail-Datenbank des Empfängers auf dem gleichen Server, so wird eine Nachricht vom Router-Prozess direkt dort abgeliefert. Liegt die Mail-Datenbank auf einem anderen Server, so wird eine Nachricht an dessen Mail.box und von dort über den Router-Prozess des anderen Servers an die Mail-Datenbank weitergeleitet.

Bestehen innerhalb einer Domäne unterschiedliche Domino-Netzwerke, so müssen zwei Verbindungsdokumente erstellt werden (eins für jede Richtung).



SERVER CONNECTION: miri/wse-edv/de to oli/V

Basics | Replication/Routing | Schedule | Comments | Administration

Basics

Connection type:	Local Area Network
Source server:	miri/wse-edv/de
Source domain:	wse-edv
Use the port(s):	TCPIP
Usage priority:	Normal
Destination server:	oli/WSE3/de
Destination domain:	WSE3
Optional network address:	

Replication

Replication task:	Enabled
Replicate databases of:	Low & Medium & High priority
Replication Type:	Pull Push
Files/Directories to Replicate:	(all if none specified)
Replication Time Limit:	minutes

Routing

Routing task:	Mail Routing
Route at once if:	5 messages pending
Routing cost:	1
Router type:	Push Only

Verbindungsdokument

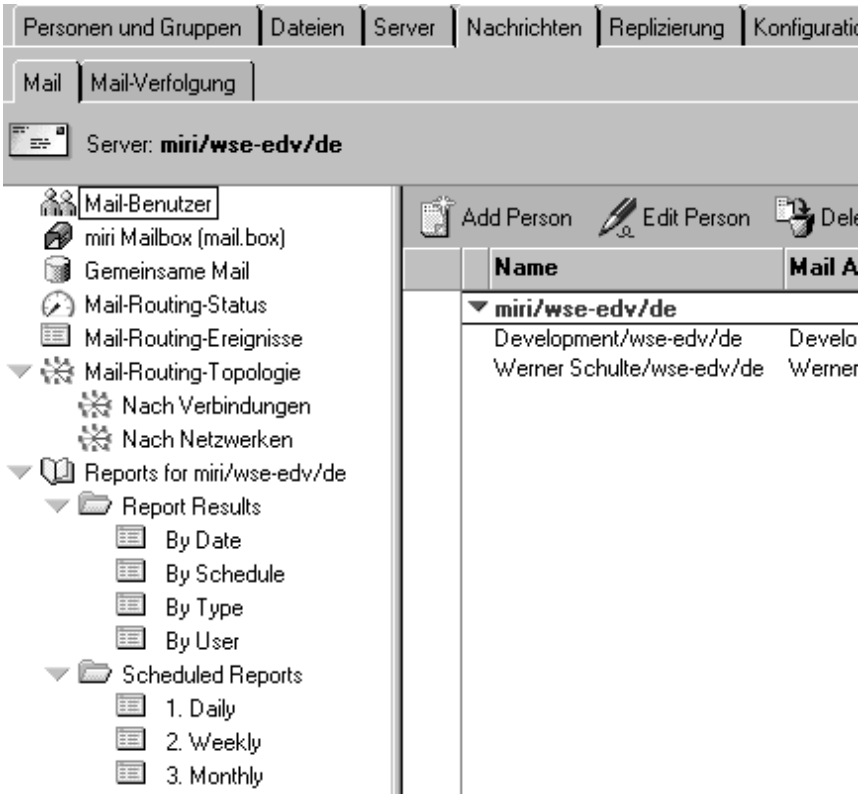
In den Verbindungsdokumenten wird geregelt, wie die Server miteinander verbunden sind, welche Replikation vorgenommen werden soll und wann die Replikation gestartet wird.

Sollen Server aus unterschiedlichen Domänen miteinander kommunizieren, so unterscheidet Domino zwischen benachbarten und fremden Domänen. Fremde Domänen sind dadurch gekennzeichnet, dass sie nur über eine benachbarte Domäne erreicht werden können. Je nach Domänenart muss in diesem Fall ein Domänendokument für eine benachbarte bzw. eine fremde Domäne erstellt werden. Bei den fremden Domänen wird zusätzlich unterschieden, ob Mail- oder Nicht-Mail-Systeme (Pager oder Fax) verwendet werden sollen.

Diese Seite ist zur Zeit nicht belegt.

7.2 Nachrichtenverwaltung im Administrator-Client

Das Register “Nachrichten” im Administrator-Client stellt Werkzeuge zur Verfügung, mit denen Mail-Informationen gesammelt und Einstellungen vorgenommen werden können.

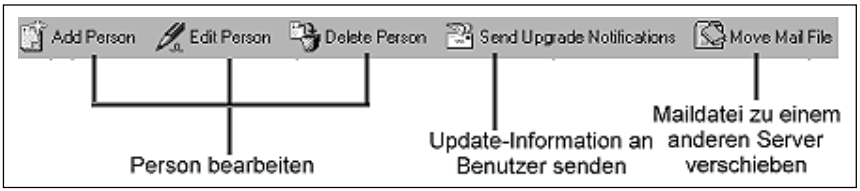


Das Register „Nachrichten“ des Administrator-Clients

Die verfügbaren Objekteinträge auf der linken Seite gliedern sich in

- Mail-Benutzer

  Hier können Benutzer im Domino-Verzeichnis verwaltet werden.



Aktionen zur Verwaltung von Mail-Benutzern

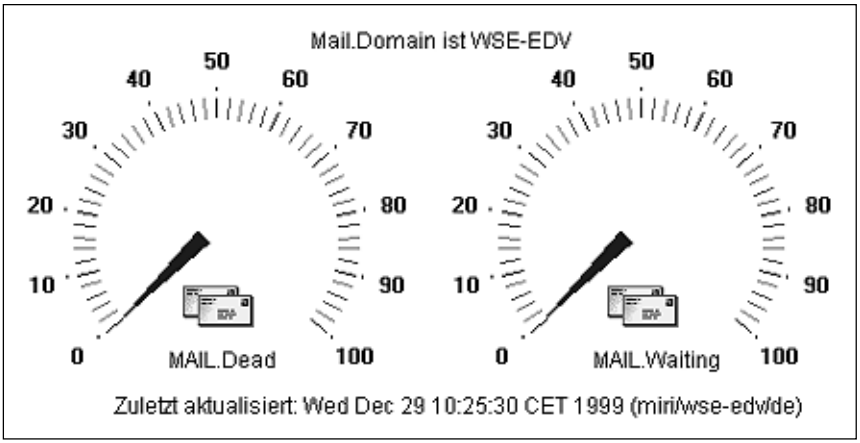
- Mailbox des Servers

  Ansicht der Mails, die in der Datenbank „Mail.box“ zur Weiterleitung anstehen.

- Gemeinsame Mail

  Zeigt Informationen zu den Dokumenten in einer gemeinsamen Mail-Datenbank an, wenn der Server eine solche verwendet.

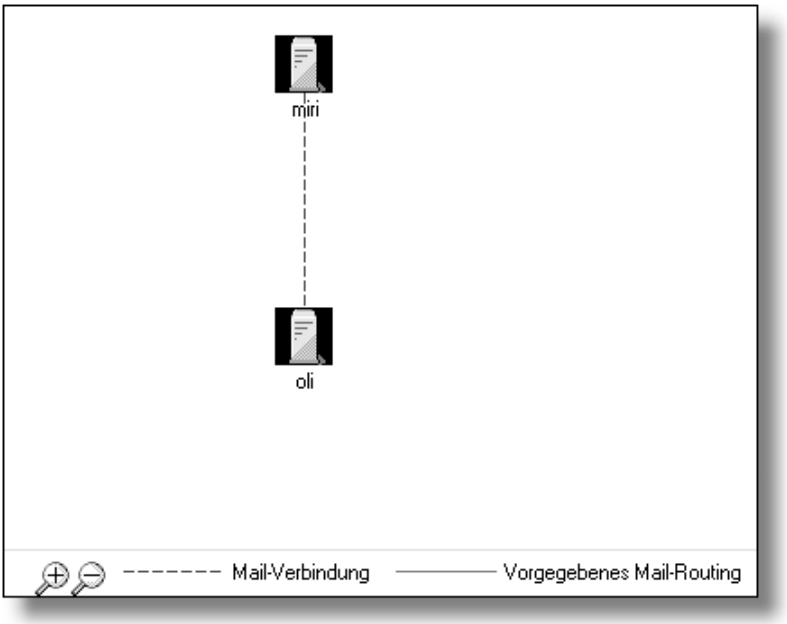
- Mail-Routing-Status
  Grafische Anzeige der Datenbank „Mail.box“.



Mail-Routing-Status

- Mail-Routing-Ereignisse
  Dokumente mit Mail-Ereignissen aus der Datenbank “Log.nsf”

- Mail-Routing-Topologie
  Grafische Darstellung der Server-Verbindungen.

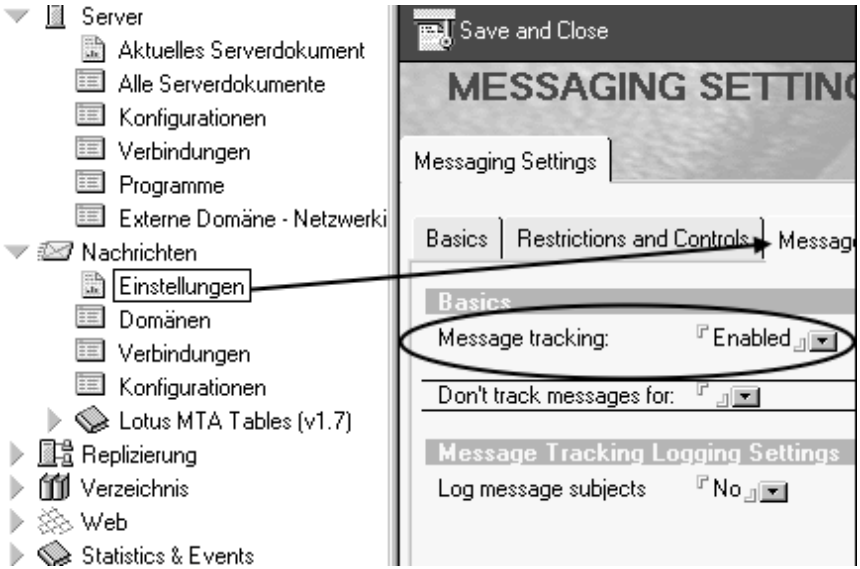


Mail-Routing-Topologie

- Server-Auswertungen

Im Unterabschnitt “Mail-Verfolgung” können Einstellungen für die Verfolgung und Protokollierung der Weiterleitung von Nachrichten vorgenommen werden. Damit solche Verfolgungsabfragen gespeichert werden können, muss zunächst die Mail-Überwachung für den Server gestartet werden. Die Angaben dazu können über

das Register ”Konfiguration / Nachrichten / Einstellungen” im Unterabschnitt „Router/SMTP-Mail-Verfolgung“ gemacht werden. Das Feld “Mail-Verfolgung” muss auf “Aktiviert” gesetzt werden. Außerdem kann festgelegt werden, welche Mails und Themen in welchen Zeitabständen protokolliert werden sollen.



Mail-Verfolgung aktivieren

Der Server legt jetzt eine neue Datenbank mit dem Namen “MTSTORE.NSF” an und startet einen zusätzlichen Prozess (mtc), der die Mail-Informationen sammelt.

Sobald die neue Datenbank vorhanden ist, können Mail-Verfolgungsabfragen definiert werden.

Mail-Verfolgungsabfrage definieren

8

Datenbanken und Replikation

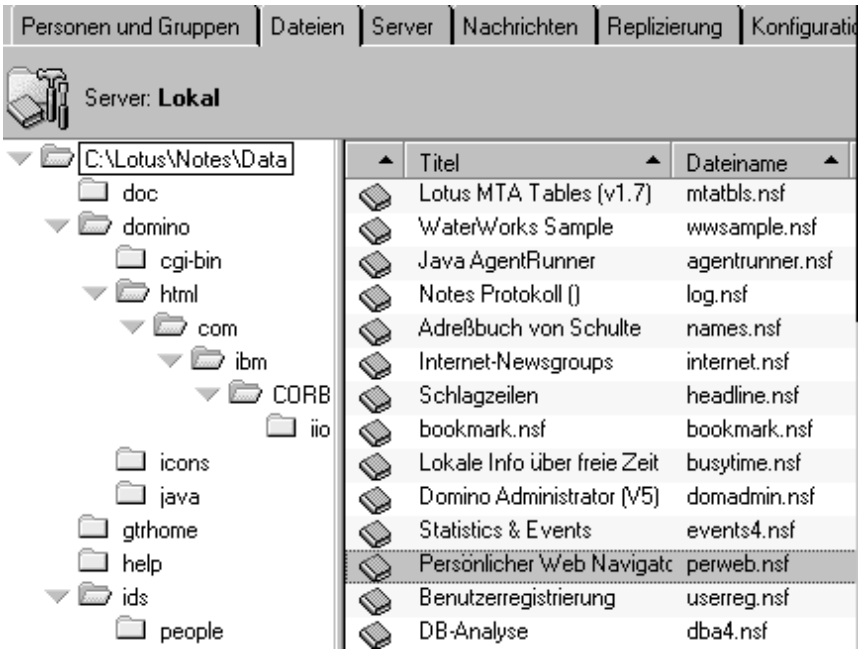
Datenbanken sind die Basis für die Speicherung von Daten und Programmen im Domino-System. Die Verwaltung der Datenbanken beinhaltet die Datensicherung, Rechteverwaltung, Datenverteilung durch Replikation, die Überwachung des Plattenplatzes und der Datenbankgröße, sowie die Korrektur aufgetretener Datenbankfehler. Datenbanken werden als Bestandteil des Systems bei der Installation von Domino und Notes erstellt. Andere werden

später als Kopie eingefügt oder von Benutzern, Administratoren und Entwicklern erstellt. Je nach Ursprung der Datenbank sind unterschiedliche Benutzungs- und Verwaltungsrechte mit den Datenbanken verbunden. Die Verwaltung der Rechte an Datenbanken wird im Rahmen des Sicherheitskonzeptes von Domino besprochen. An dieser Stelle soll die technische Bearbeitung und Überwachung der Datenbanken besprochen werden.

8.1 Datenbankadministration

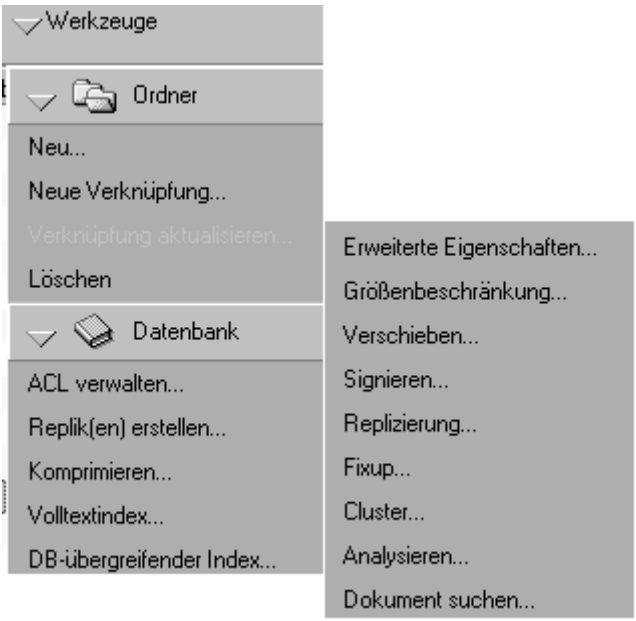
Über das Register „Dateien“ des Administrator-Clients kann eine Auflistung der Datenbanken eines Servers bzw. einer Arbeitsstation angezeigt werden. Die Auflistung kann unterschiedliche Inhalte haben:

- nur Datenbanken
- nur Datenbankvorlagen
- alle Dateien
- eine benutzerdefinierte Auswahl



Auflistung der Datenbanken

Durch Doppelklick auf die Zeile der Datenbank wird sie geöffnet. Wichtiger sind aber die Werkzeuge, die für das Register angezeigt werden. Mit den angezeigten Maßnahmen können eine oder auch mehrere Datenbanken verarbeitet werden.



Werkzeuge für die Bearbeitung von Datenbanken

Im ersten Abschnitt der Werkzeuge werden Ordneraktionen aufgeführt:

- Neu...

  Anlegen eines neuen Verzeichnisses unter dem ausgewählten Verzeichnis.
- Neue Verknüpfung

  Verzeichnis außerhalb des Data-Verzeichnisses zur Einbindung in die Datenbankanzeige

- Verknüpfung aktualisieren

  Nur verfügbar, wenn eine Verknüpfung besteht.

- Löschen

  Verzeichnis löschen.

Der Abschnitt „Datenbank“ enthält die Werkzeuge zur Bearbeitung einzelner oder mehrerer Datenbanken bzw. Datenbankschablonen:

- ACL verwalten

  Leider können mit dieser Aktion keine vorhandenen ACL-Einträge angezeigt werden. Sie ist aber trotzdem eine große Hilfe, z.B. dann, wenn vielen Datenbanken eine neue Gruppe oder Rolle hinzugefügt werden soll.

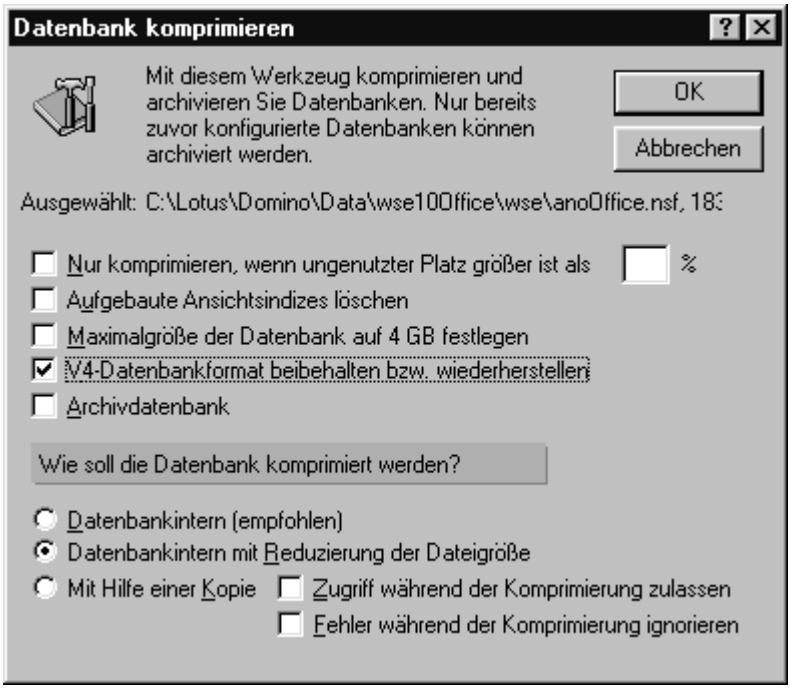
ACL verwalten

- Replik(en) erstellen

  Auf mehreren Servern können Repliken einer Datenbank erstellt werden.

- Komprimieren

  Eine oder mehrere Datenbanken nach Vorgabe komprimieren.



Datenbank(en) komprimieren

- Volltextindex

  Erstellt und aktualisiert Volltext-Indices zu Datenbanken.

- Datenbankübergreifender Index

  Datenbank in einen Index über mehrere Datenbanken hinweg aufnehmen.

- Erweiterte Datenbankeigenschaften

  Ändert die erweiterten Eigenschaften einer oder mehrerer Datenbanken.

- Größenbeschränkung

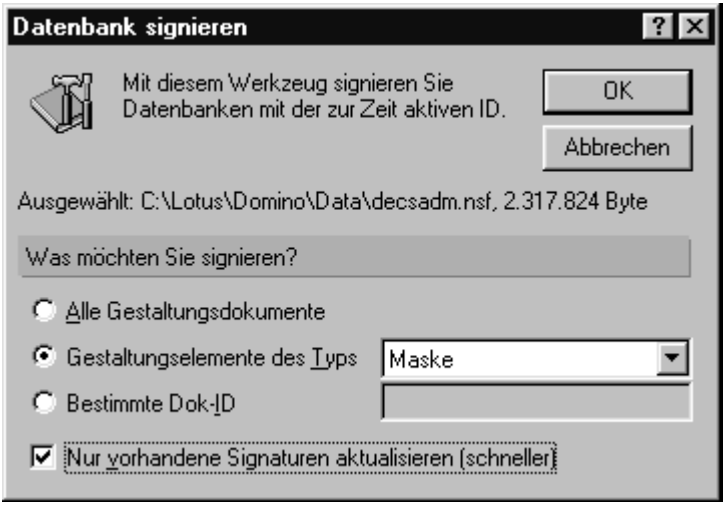
  Erlaubt die Beschränkung der verwendbaren Datenbankgröße.

- Verschieben

  Datenbanken auf einen anderen Server schieben.

- Signieren

  In der Signatur ist der Ersteller eines Objektes hinterlegt. Bei der Verwendung des Objektes wird anhand der Signatur geprüft, ob eine Aktion ausgeführt werden darf. Mit dem Werkzeug „Datenbank signieren“ kann einem oder mehreren Objekten einer Datenbank die Signatur des aktuellen Benutzers gegeben werden.



Datenbank signieren

- Replizieren

  Aktivieren oder Deaktivieren der Replizierung von Datenbanken.

- Fixup

  Beschädigte Datenbanken manuell reparieren.

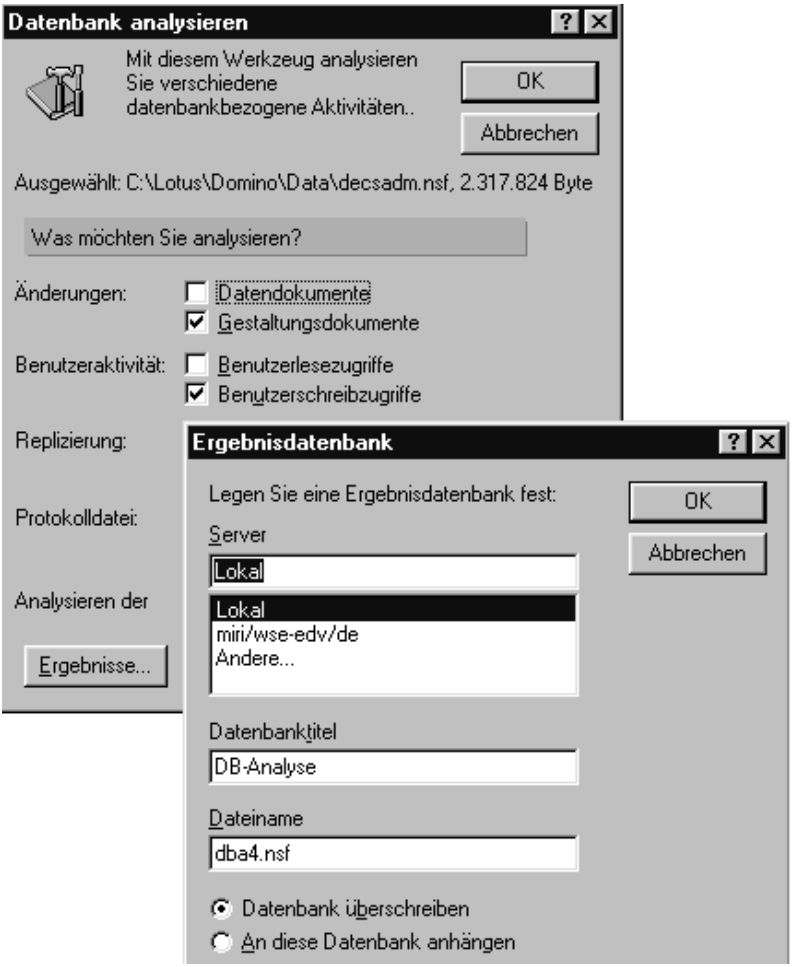
Datenbank-Fixup

- Cluster

  Übernimmt die aktuelle Datenbank in ein Cluster.

- Analyse

  Nicht die Datenbank wird analysiert, sondern Aktivitäten im Zusammenhang mit der Datenbank werden untersucht und in eine Ergebnisdatenbank abgespeichert.



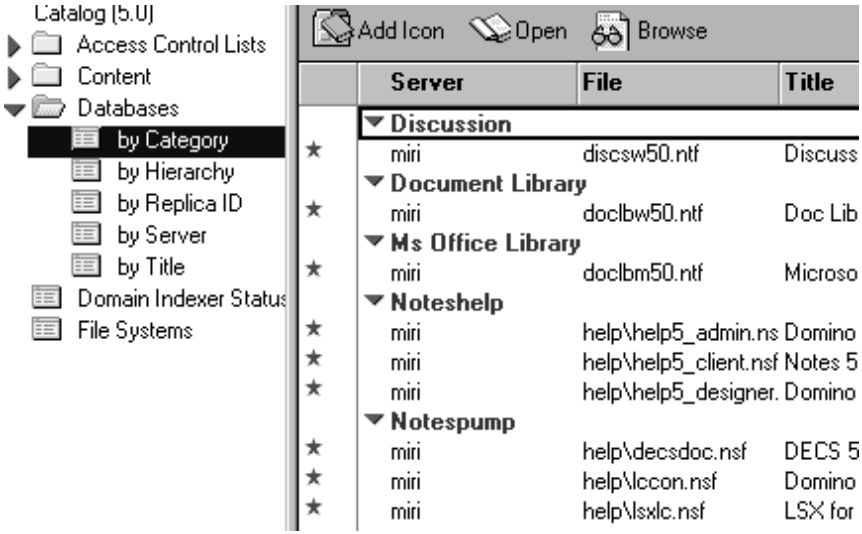
Datenbankanalyse

- Dokument suchen

  Anhand der Dok-ID oder der Universal-ID nach einem Dokument in den gekennzeichneten Datenbanken suchen.

8.2 Der Datenbank-Katalog

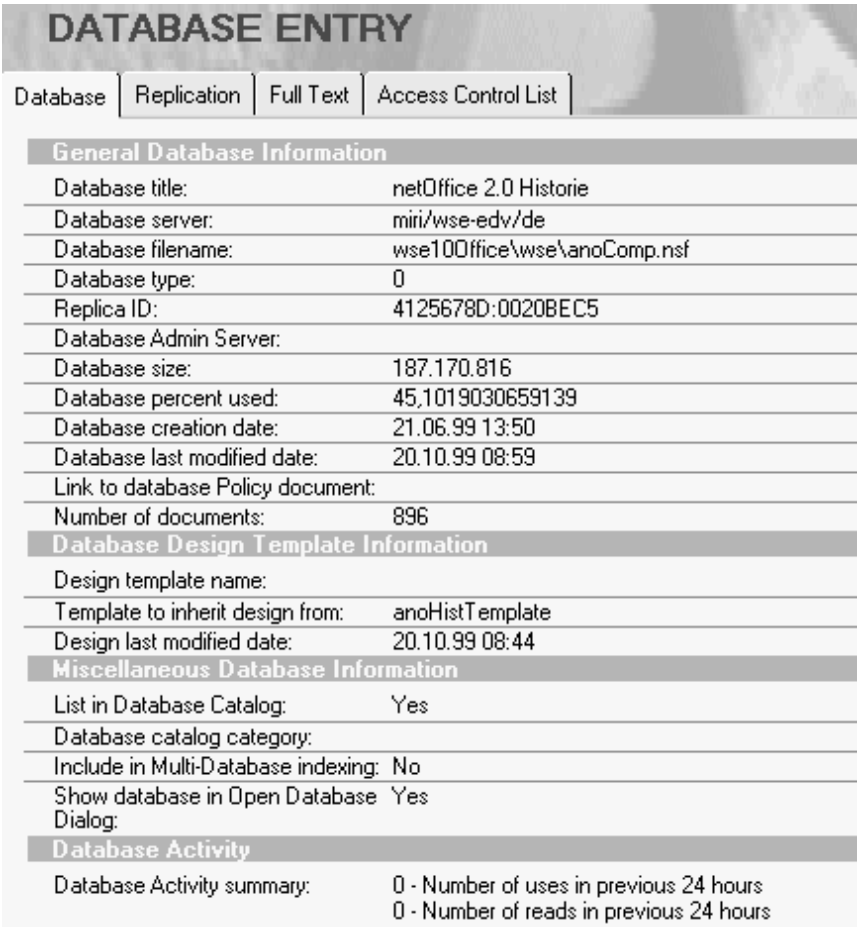
Bei den Eigenschaften einer Datenbank wird standardmäßig hinterlegt, dass sie in den Datenbank-Katalog aufgenommen wird. Es handelt sich bei diesem Katalog um eine Datenbank mit dem Namen „Catalog.nsf“, die von einem Prozess namens „Catalog“ auf dem neuesten Stand gehalten wird.



Der Datenbank-Katalog

Für jede Datenbank enthält diese Datenbank ein Dokument. Die Dokumente können über verschieden Ansichten angezeigt werden. Die Dokumente enthalten Informationen über

- die Datenbankeigenschaften und die Zusammenfassung der Datenbankaktivitäten



DATABASE ENTRY

Database | Replication | Full Text | Access Control List

General Database Information	
Database title:	netOffice 2.0 Historie
Database server:	miri/wse-edv/de
Database filename:	wse10Office\wse\anoComp.nsf
Database type:	0
Replica ID:	4125678D:0020BEC5
Database Admin Server:	
Database size:	187.170.816
Database percent used:	45,1019030659139
Database creation date:	21.06.99 13:50
Database last modified date:	20.10.99 08:59
Link to database Policy document:	
Number of documents:	896
Database Design Template Information	
Design template name:	
Template to inherit design from:	anoHistTemplate
Design last modified date:	20.10.99 08:44
Miscellaneous Database Information	
List in Database Catalog:	Yes
Database catalog category:	
Include in Multi-Database indexing:	No
Show database in Open Database Dialog:	Yes
Database Activity	
Database Activity summary:	0 - Number of uses in previous 24 hours 0 - Number of reads in previous 24 hours

Datenbankeigenschaften

- Replikationseinstellungen
- Informationen zum Volltext-Index

Replication Settings	
Replication disabled:	No
Receive replication summaries:	No
Send deletions:	No
Send title and catalog information:	Yes
Replication priority:	Low
Remove documents not modified:	No in last 0 days

Full Text Index Information	
Database full text indexed:	No
Number of bytes indexed:	bytes
Full text index last updated:	

Replikation und Volltext-Index

- Zugriffskontroll-Liste

  Auflistung der genauen Rechteverteilung an einer Datenbank einschließlich der Aktionen und Funktionen

Access Control List						
		Actions				
	Names	CrDoc	DlDoc	PerAg	PerFld	ShrFld
Managers:	WSE Development/WSE3/de	1	1	1	1	1
	LocalDomainServers	1	1	1	1	1
	Development/wse-edv/de	1	1	1	1	1
	Werner Schulte/wse-edv/de	1	1	1	1	1
	Werner Schulte/WSE3/de	1	1	1	1	1
Designers:						
Editors:						
Authors:						
Readers:						
Depositors:						
No Access:	-Default-	0	0	0	0	0

Legend:
CrDoc = Create documents
DlDoc = Delete documents
PerAg = Create personal agents
PerFld = Create personal folders/views
ShrFld = Create shared folders/views
LscAg = Create Lotusscript/Java agents
RdPub = Read public documents
WrPub = Write public documents

Zugriffskontroll-Liste

8.3 Replikation

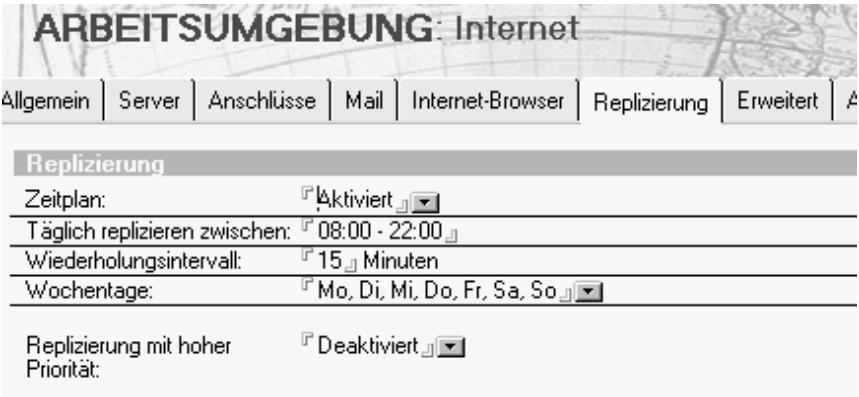
Eine der ältesten und wichtigsten Funktionen in Lotus Domino ist die Replikation. Während bei relationalen Datenbanken weitestgehend vermieden wird, Daten mehrfach vorzuhalten, ist es eine typische Domino-Eigenschaft, Kopien von Datenbanken, also mehrere Versionen der Daten zu verwenden (Lokale Repliken auf Arbeitsstationen bzw. Mobilrechnern). Damit die Daten nach einer Änderung in allen Datenbankkopien wieder angeglichen werden, synchronisiert Domino die Datenbanken in bestimmten Abständen und passt die Daten entsprechend an. Damit die Synchronisation erfolgreich sein kann, arbeitet Domino sowohl bei den Datenbanken als auch bei den Dokumenten mit Identifikationsnummern, den IDs. Eine Replikation ist möglich zwischen einer Arbeitsstation und einem Server oder zwischen Servern. Eine direkte Replikation zwischen Arbeitsstationen ist nicht möglich.

8.3.1 Automatische Replikation

Mit dem Start des Domino-Servers wird auch der Replikator-Prozess aktiviert. Er wartet auf ein manuelles oder im Zeitplan enthaltenes Replikationsereignis. Wird ein solches Ereignis ausgelöst, so verwendet der Prozess die Replikationseinstellungen der Datenbanken und aktualisiert deren Inhalte.

8.3.1.1 Die Replikation zwischen Arbeitsstation und Server

Damit die Datenbanken einer Arbeitsstation regelmäßig mit einem Server abgeglichen werden, wird in einer Arbeitsumgebung, die mit diesem Server verbindet, ein Zeitplan für die Replizierung eingerichtet.

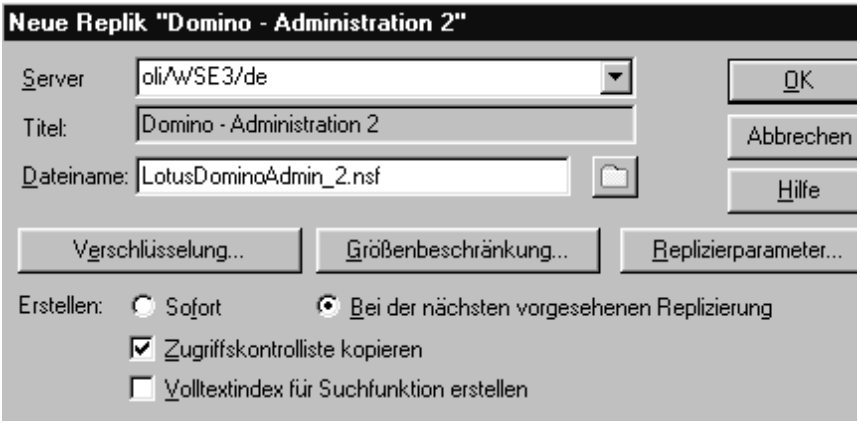


Register „Replizierung“ in einer Arbeitsumgebung

Nachdem im Feld „Zeitplan“ der Wert „Aktiviert“ eingetragen wurde, kann der eigentliche Zeitplan eingetragen werden.

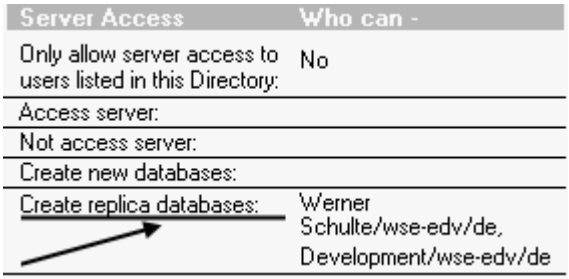
Damit die einzelnen Datenbanken tatsächlich repliziert werden, muss von jeder Datenbank eine Replik auf der Arbeitsstation bzw. umgekehrt auf dem Server angelegt werden.

Zur Anlage einer Replik verwenden Sie das Menü „Datei / Replizierung / Neue Replik“. Es wird ein Dialog angezeigt, in dem die neue Replik der Datenbank definiert werden kann.



Neue Replik

Soll die Replik auf einem Server angelegt werden, so muss der Benutzer, der die Replik anlegt, das Recht haben, auf dem Server Repliken zu erstellen.

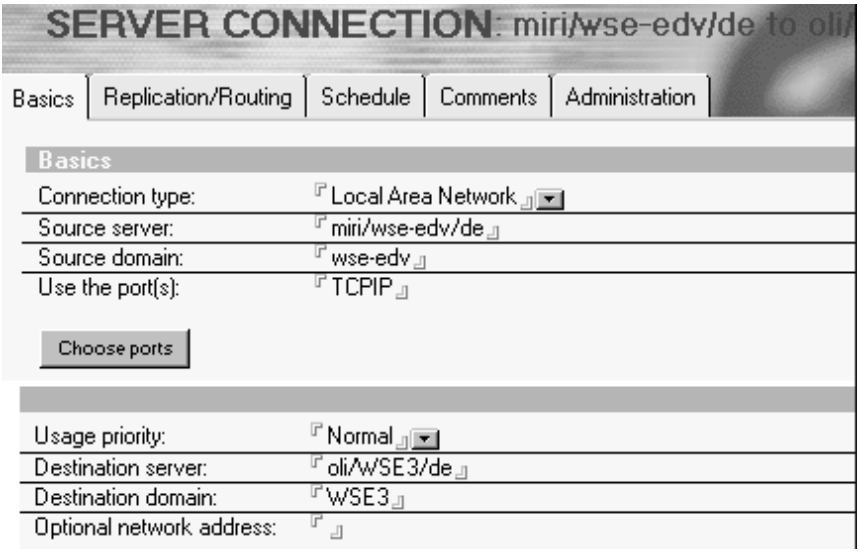


Server-Rechte

Sobald die beiden Repliken vorhanden sind, werden sie über den Zeitplan der Arbeitsumgebung automatisch aktualisiert.

8.3.1.2 Server-zu-Server-Replikation

Die Replikation zwischen Servern wird über Verbindungsdokumente gesteuert. Im Register „Allgemein“ werden die Server und der Anschluss für die Verbindung angegeben.



Server-Verbindungsdokument

Im Register „Routing/Replizierung“ finden sich die Eintragungen für die eigentliche Replikation. Im Feld „Replizierungsfunktion“ wird die Replizierung aktiviert. Über den Replizierungstyp wird festgelegt, wie die Replizierung ablaufen soll:

- Pull-Pull

  Der erste Server holt alle Änderungen und teilt dann dem zweiten Server mit, dass er die Änderungen holen kann. Der zweite holt nun die Änderungen des ersten Servers.

- Pull-Push

  Der erste Server holt die Änderungen des zweiten Servers und schreibt seine Änderungen in die Datenbank dieses Servers. Diese Methode ist der Vorgabewert.

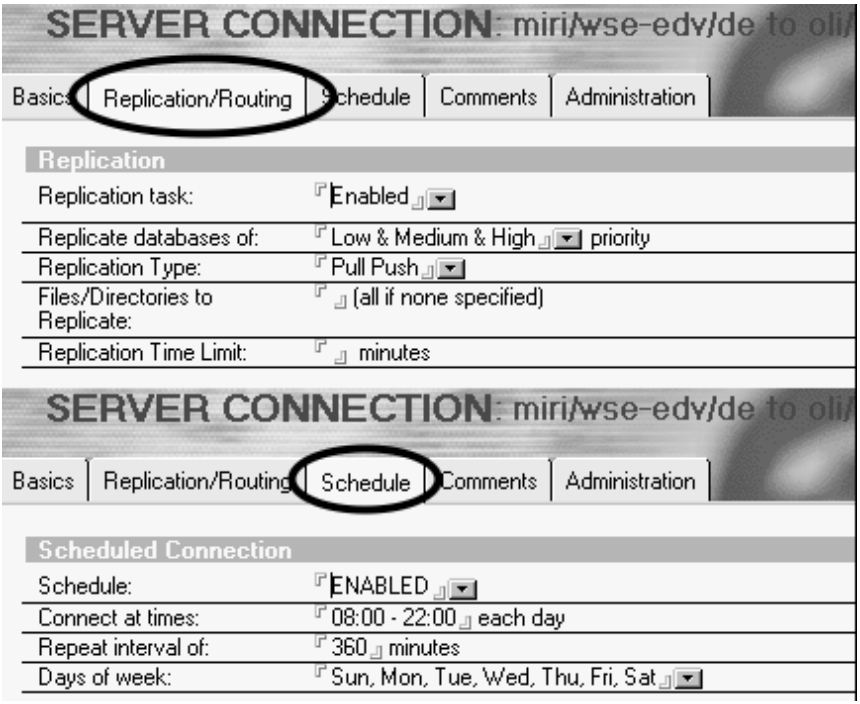
- Nur Pull

  Der eine Server holt nur die Änderungen des anderen Servers.

- Nur Push

  Der eine Server schreibt seine Änderungen in die Datenbank des anderen Servers.

Die zu replizierenden Datenbanken können auf bestimmte Datenbanken oder Verzeichnisse beschränkt werden. Die Einträge werden durch Semikolon getrennt. Verzeichnisse werden vom Data-Verzeichnis aus definiert (z.B. net50Str.ntf; wse\netOffice). Auch die Zeit, innerhalb der die Replizierung durchgeführt sein muss, kann eingetragen werden.



Replizierungsangaben im Verbindungsdokument

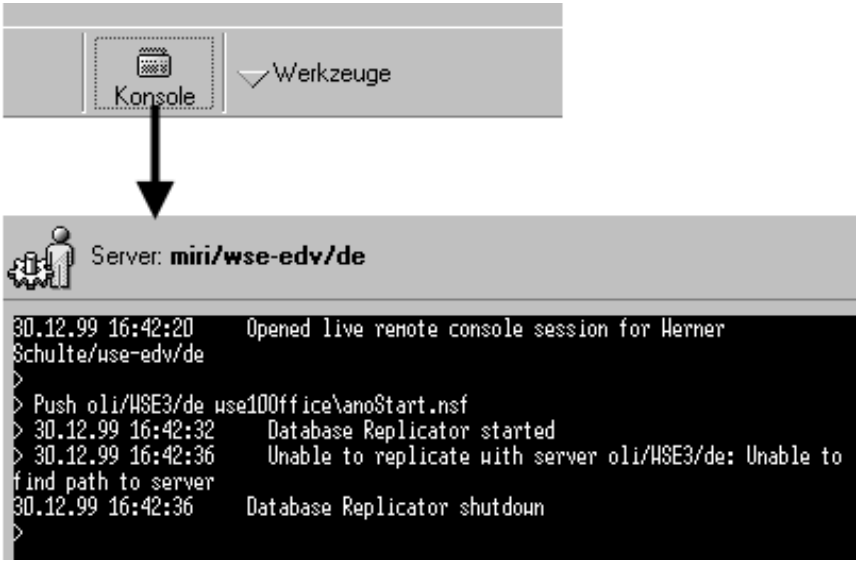
Im Abschnitt „Zeitplan“ wird schließlich definiert, wann der Replikator-Prozess aktiv sein soll.

Damit die Server auch berechtigt sind, die Datenbanken zu lesen und in ihnen zu schreiben, sind in den Zugriffskontroll-Listen der Datenbanken die Server mit den entsprechenden Rechten aufzuführen. Zur Vereinfachung dieser Berechtigung sollten alle Server der eigenen Domäne in der Gruppe „LocalDomainServers“ und in den Zugriffskontroll-Listen mit Manager-Rechten aufgeführt sein.

Diese Seite ist zur Zeit nicht belegt.

8.3.2 Manuelle Replikation

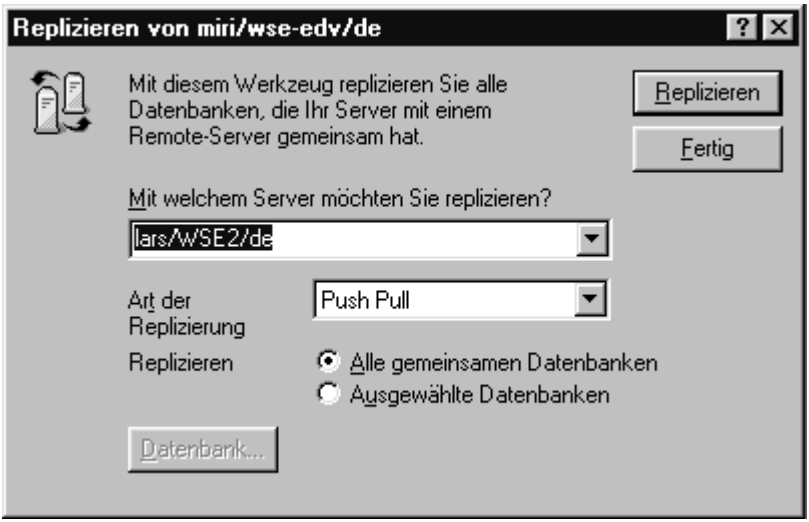
Eine manuelle Replikation zwischen Servern kann über die Domino-Konsole oder den Administrator-Client erfolgen.



Server-Konsol-Befehl „Push“

In der Domino-Konsole werden die Befehle Replicate, Push Server oder Pull verwendet.

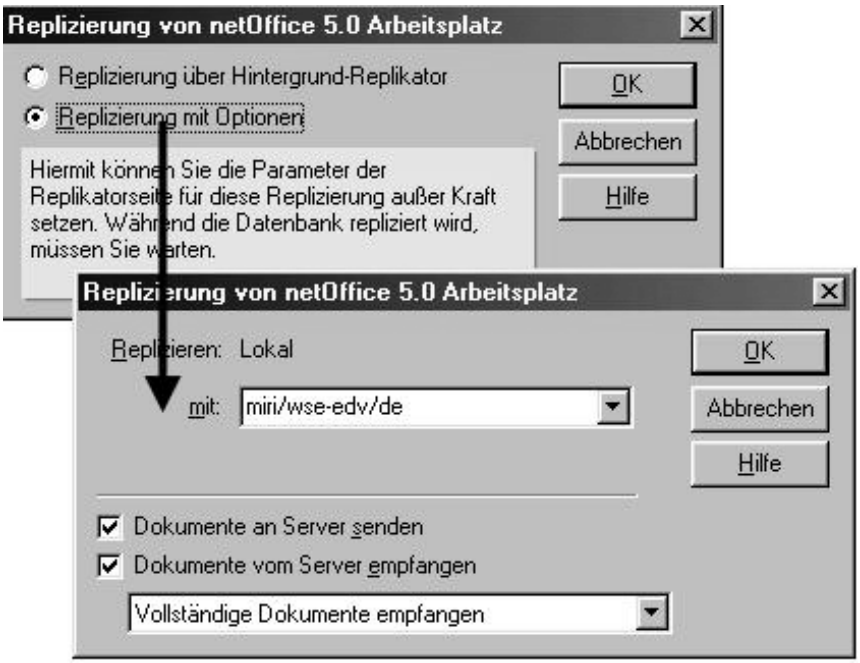
Über den Administrator-Client kann die Replikation auch direkt angestoßen werden.



Replizieren über den Administrator-Client

Dazu werden im Register „Server“ in der Werkzeugleiste der Abschnitt „Server“ und der Eintrag „Replizieren“ verwendet.

Auch von einer Arbeitsstation aus kann eine manuelle Replizierung angestoßen werden. Über das Menü „Datei / Replizierung / Replizieren“ wird ein Dialog geöffnet, in dem der Server ausgewählt wird, mit dem die aktuelle Datenbank repliziert werden soll.

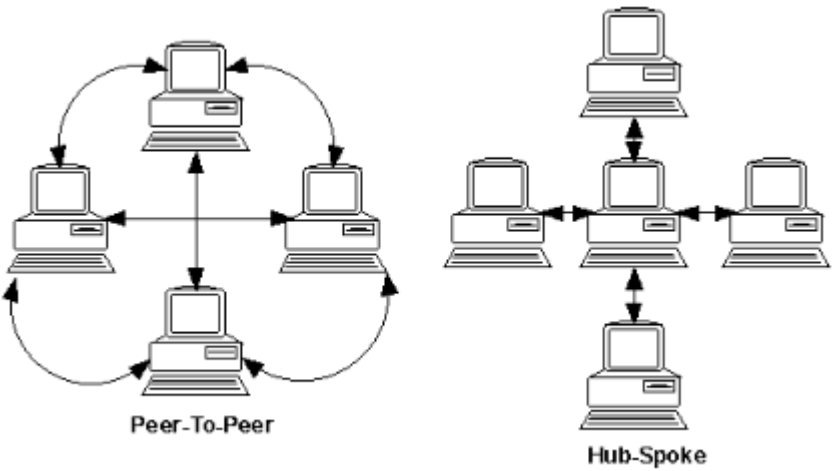


Replizieren von der Arbeitsstation aus

Diese Seite ist zur Zeit nicht belegt.

8.3.3 Server-Topologien

In der Praxis kommt es häufig vor, dass Datenbanken auf mehreren Servern vorgehalten werden müssen. Damit stellt sich die Frage, in welcher Reihenfolge die Server miteinander replizieren sollen. Grundsätzlich gibt es zwei Prinzipien, wie die Server miteinander verbunden werden können. Die erste Verbindungsart „Peer-To-Peer“ bedeutet, dass jeder Server mit jedem anderen Server verbunden wird. Das bedeutet, dass sehr viele Replikationsvorgänge stattfinden und deren Koordination entsprechend kompliziert ist. Besser ist das sog. Hub-Spoke-Prinzip, bei dem alle Server mit einem zentralen Server verbunden werden.



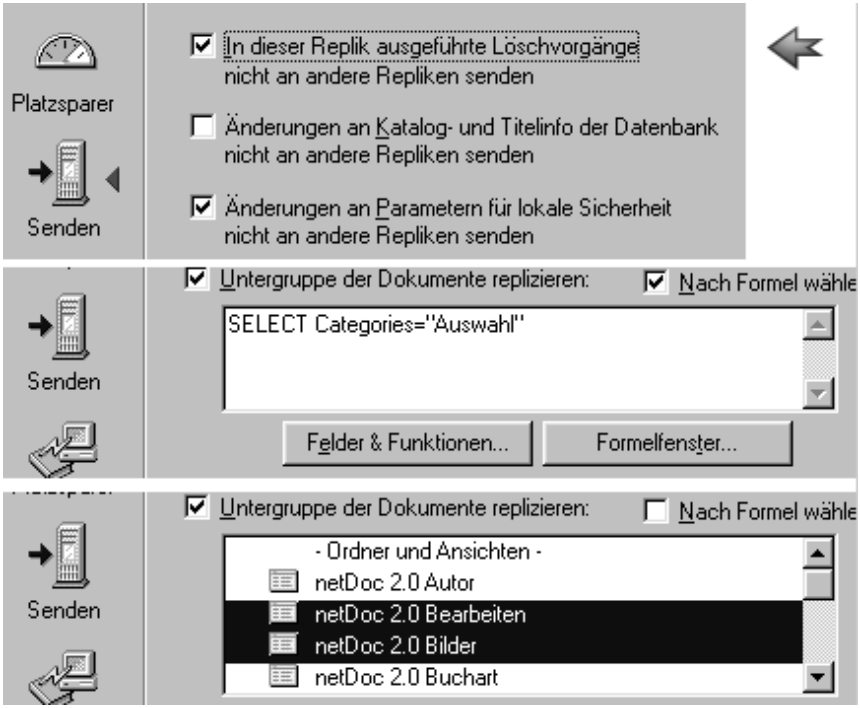
Server-Topologien

Die Anzahl der Verbindungen ist hier geringer und entsprechend einfacher ist die Koordination der Replizierung.

Diese Seite ist zur Zeit nicht belegt.

8.3.4 Replikationseinstellungen

Standardmäßig werden alle Änderungen zwischen zwei Replikaten einer Datenbank ausgetauscht. Häufig ist es aber nicht erwünscht, dass alle Informationen in beiden Versionen der Datenbank enthalten sind. Es ist auch denkbar, dass nicht alle Änderungsarten ausgetauscht werden sollen. Für solche Anforderungen können bei der Datenbank Replikationsparameter eingestellt werden.



Einschränkungen der Replikation

Über das Menü “Datei / Replizierung / Parameter” können die Einstellungen für die Replikation der Datenbank vorgenommen werden. In den Beispielen der obigen Abbildung werden folgende Einschränkungen gezeigt:

- Löschvorgänge nicht weitergeben

  Diese Einstellung dient dazu, Löschungen, die auf einer mobilen oder lokalen Arbeitsstation vorgenommen wurden, nicht auf den Server zu übernehmen.

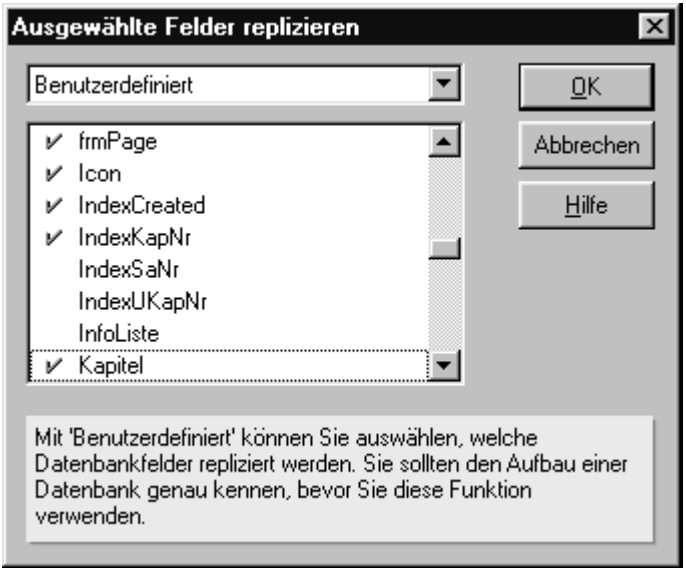
- Dokumente auf eine Auswahl beschränken

  So könnte z.B. die Replikation auf den Arbeitplatz eines Außendienstmitarbeiters auf dessen Gebiet beschränkt werden.

- Replikation einer oder mehrerer Ansichten

  Nur Dokumente, die in einer bestimmten Ansicht enthalten sind (also z.B. Dokumente, die von einer bestimmten Person erstellt wurden) werden repliziert.

Die Möglichkeiten, die Replikationsinhalte zu beschränken, gehen so weit, dass nur die Inhalte bestimmter Felder repliziert werden.

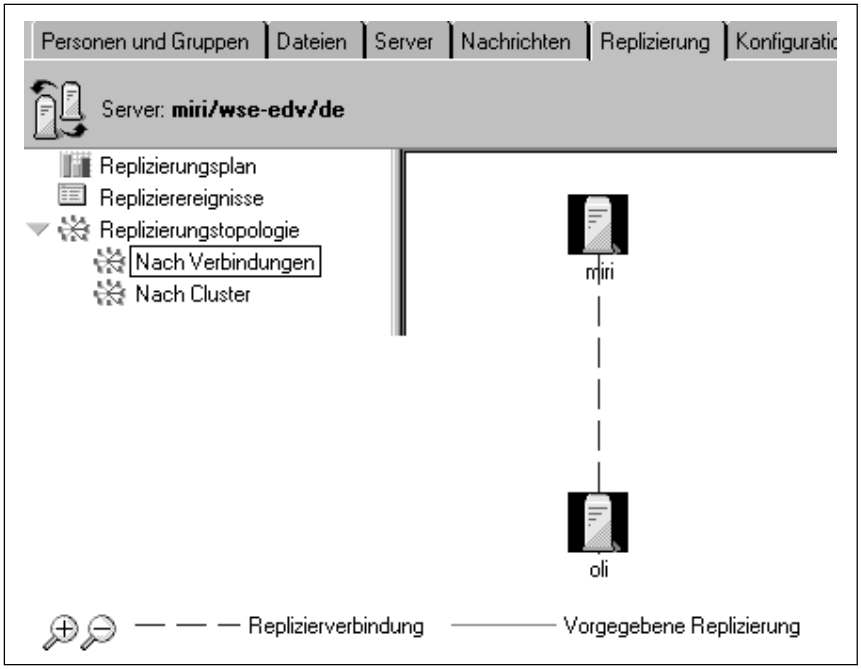


Ausgewählte Felder replizieren

Diese Seite ist zur Zeit nicht belegt.

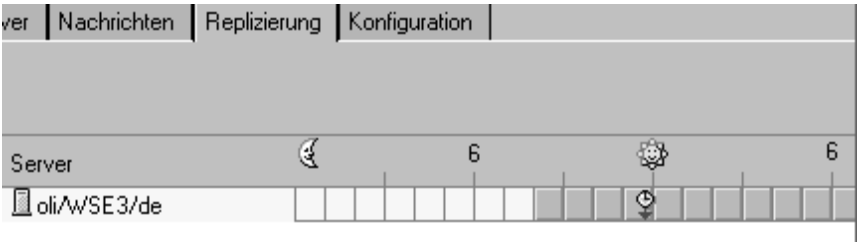
8.3.5 Überwachung der Replikation

Für die Überwachung der Replizierung stellt der Administrator-Client verschiedene Werkzeuge bereit. Im Register "Replizierung" kann die Replizierierungstopologie als grafische Darstellung abgerufen werden.



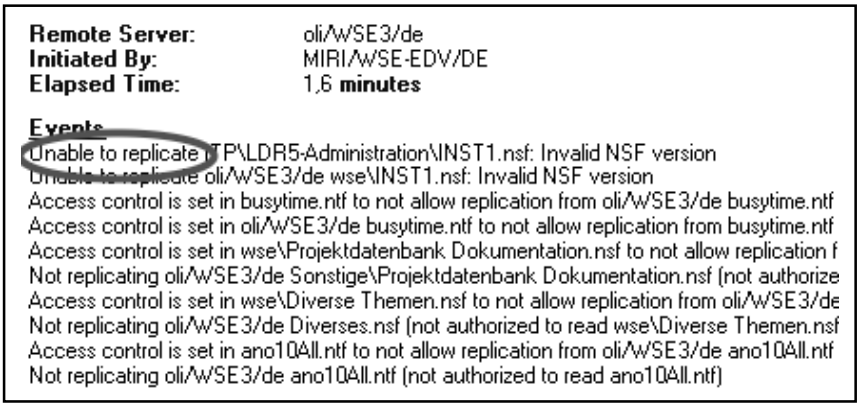
Replizierungstopologie

Im Replizierungsplan wird der geplante Zeitraum und der aktuelle Stand der Replizierung mit den verschiedenen Servern dargestellt.



Replizierungsplan

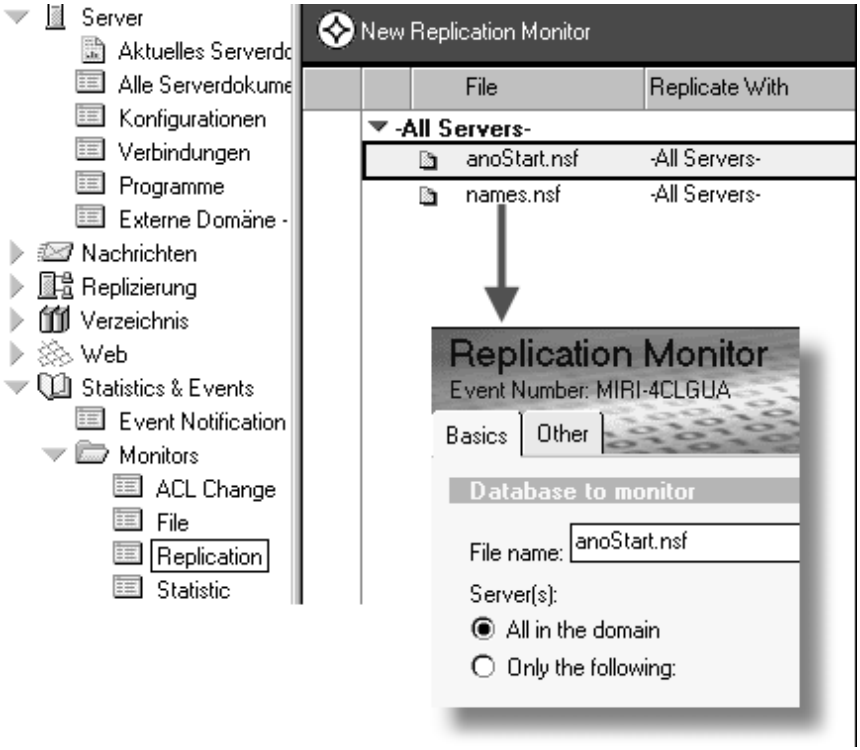
In der Datenbank „Log.nsf“ schließlich werden Replikationsvorgänge gesammelt und im Administrator-Client unter “Replizierereignisse” angezeigt.



Replizierereignisse

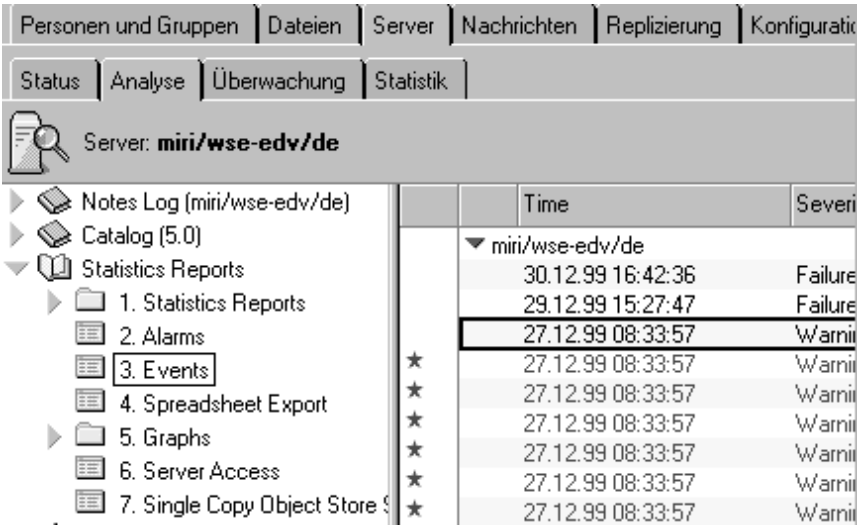
Anhand der Hinweise in diesem Protokoll können Fehler beseitigt und eine einwandfreie Replikation gewährleistet werden.

Eine weitere Möglichkeit bietet das Erstellen eines Replizierungsmonitor-Dokumentes.



Replizierungs-Überwachung

Informationen über fehlgeschlagene Replizierung werden als Ereignisse im Abschnitt “Analyse” des Registers “Server” des Administrator-Clients angezeigt.



Server-Ereignisse

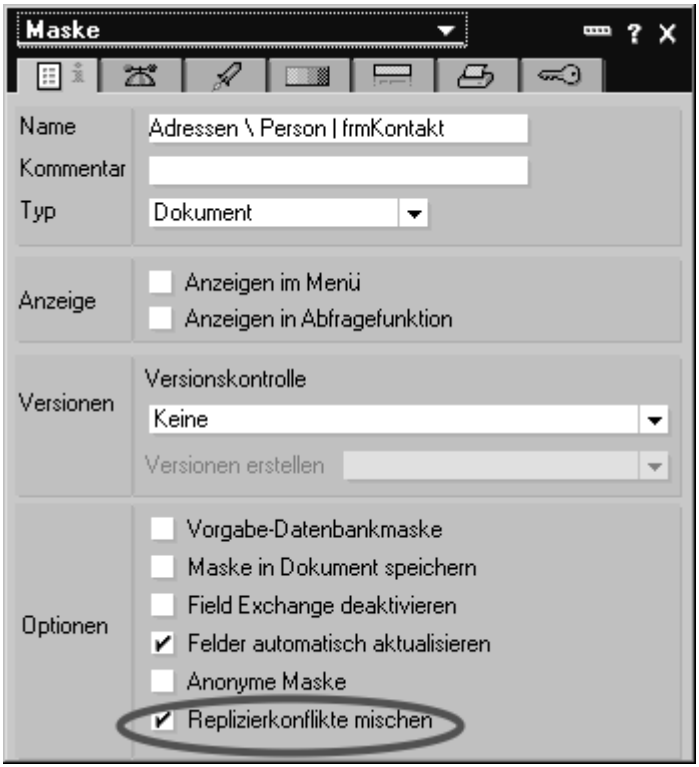
8.3.6 Speicher- und Replizierkonflikte

Ein Speicher- und Replizierkonflikt entsteht immer dann, wenn zwei Benutzer zur gleichen Zeit an einem Dokument arbeiten und den Inhalt des gleichen Feldes ändern.

Wenn die Benutzer an Datenbanken arbeiten, die zur Bearbeitungszeit völlig unabhängig von einander sind, kann Domino nicht entscheiden, welche Version des bearbeiteten Dokumentes gültig sein soll. Beim Replizieren wird in dieser Situation ein Hauptdokument und ein Antwortdokument mit jeweils einer Änderungsvariante angelegt.

In der gleichen Art geht Domino vor, wenn zwei Benutzer dasselbe Dokument auf einem Server öffnen und bearbeiten. Hier handelt es sich um einen Speicherkonflikt, bei dem ebenfalls ein Haupt- und ein Antwortdokument erstellt werden.

Zur Vermeidung solcher Konflikte kann der Entwicker eine Eigenschaft der Maske verwenden: “Replizierkonflikte mischen”.



Replizierkonflikte mischen

Wenn ein Dokument in verschiedenen Feldern von unterschiedlichen Benutzern geändert wird, kann Domino die Änderungen in einem Dokument zusammenführen. Da viele Masken ein Richtext-Feld enthalten, in dem der größte Anteil des Dokumenteninhaltes

gespeichert sein kann, wird häufig von beiden Benutzern das gleiche Feld geändert. Dann entsteht auch bei der Einstellung "Replizierkonflikte mischen" ein Replizier- oder Speicherkonflikt.

Eine weitere Möglichkeit, solche Konflikte zu vermeiden, besteht darin, den Benutzern nur Autorenrechte einzuräumen. Damit wird ausgeschlossen, dass die Benutzer Dokumente anderer Benutzer ändern und die Wahrscheinlichkeit, dass ein Dokument mehrfach bearbeitet wird, sinkt.

Letztendlich können Replizier- und Speicherkonflikte in Lotus Domino nie ganz vermieden werden, da doppelte Datenhaltung eine der Grundfunktionen von Domino darstellt.

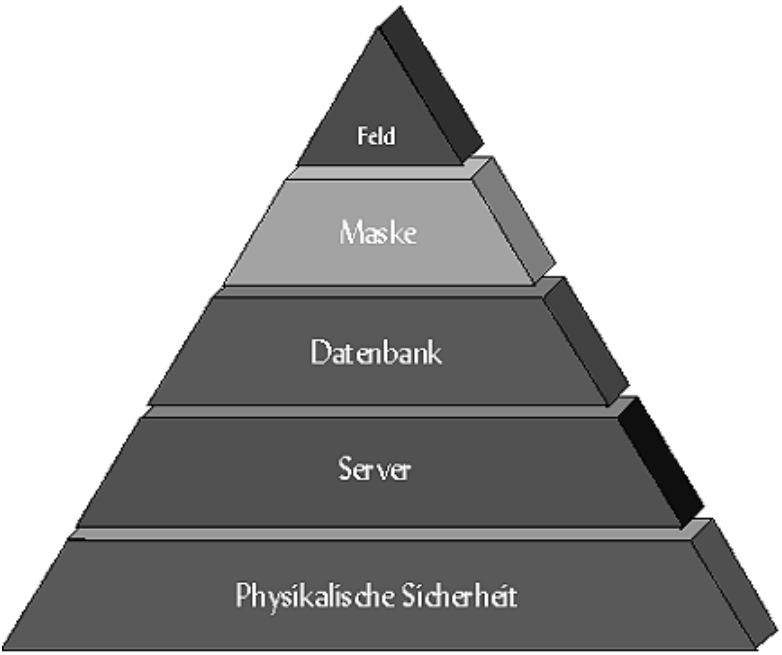
Diese Seite ist zur Zeit nicht belegt.

9

Sicherheit und Benutzerverwaltung

Jeder Benutzer, der im Domino-System arbeiten will, muss von einer Zulassungsstelle im Domino-Verzeichnis registriert sein. Er erhält eine ID-Datei, die wie ein Ausweis verwendet wird und die seine Rechte im System steuert.

Die erste Zulassungsstelle (cert.id) wird bei der Installation des ersten Domino-Servers zusammen mit der Server-ID und der ID der Administrators erstellt.



Sicherheitsstufen in Lotus Domino

Die Daten innerhalb des Systems sind auf verschiedenen Stufen gegen unbefugten Zugriff geschützt.

9.1 Sicherheitseinstellungen

Schon bei der räumlichen Sicherheit beginnen die Vorkehrungen, die getroffen werden sollten, um für die Sicherheit im Domino-System Sorge zu tragen. Wer seine Server für jedermann zugänglich macht, darf sich nicht wundern, wenn es zu unvorhergesehenen Störungen durch Geräteausfall, Systemabstürze und Beendigungen des Server-Programms kommt. Auch bei abgeschlossenen Räumen lässt es sich nicht ganz vermeiden, dass verschiedene Personen Zugang zu Server-Rechnern haben. Damit nur berechtigte Personen mit den Domino-Servern arbeiten können, sollten also auch hier noch Vorkehrungen getroffen werden. Neben mechanischen Sicherungen und Betriebssystemrechten kann dazu ein i1Konsolen-Kennwort für den Domino-Server vergeben werden. Mit Hilfe des Konsolbefehls „SET SECURE“ kann die Server-Konsole vor unberechtigtem Zugriff geschützt werden.

SET SECURE {neues Kennwort} – Kennwort setzen

SET SECURE {aktuelles Kennwort} – Kennwort aufheben

SET SECURE {aktuelles Kennwort} {neues Kennwort}
– Kennwort ändern

Das Kennwort wird in der Notes.ini verschlüsselt gespeichert:

Server_Console_Password = xxxxxxxx

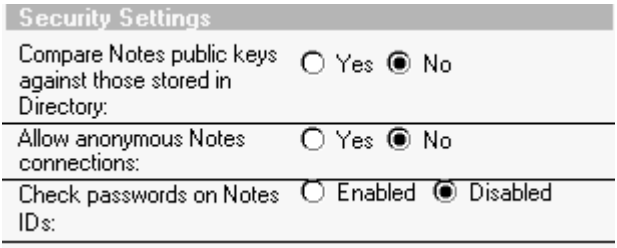
Achtung!

Wird der Eintrag gelöscht, ist die Konsole ohne Kennwort zugänglich.

Von der Server-Konsole aus kann das Sicherheitskonzept von Notes weitgehend umgangen werden, da auf dem lokalen Rechner alle Rechte änderbar sind.

9.1.1 Sicherheitseinstellungen auf dem Server

Sowohl von der Domino- als auch von der Internet-Seite aus können Einstellungen für den Server-Zugriff gemacht werden.



Sicherheitseinstellungen

Im Abschnitt „Sicherheitseinstellungen“ des Server-Dokumentes werden die ersten Prüfungen aktiviert. Die Standardeinstellungen sind sehr großzügig und sollten nach der Installation geändert werden.

- **Öffentliche Schlüssel vergleichen**
  Aktiviert den Vergleich zwischen den öffentlichen Schlüsseln der Benutzer-ID und der des Servers.

- **Anonyme Notes-Verbindungen aufbauen**
  Dieser Wert sollte auf „Nein“ stehen, damit keine Zugriffe über fremde Server möglich sind.

- **Kennwörter überprüfen**
  Zwingt die Benutzer zu einer Kennwortänderung nach einer vorgegebenen Zeit.

Der Abschnitt „Server-Zugriff“ regelt, welche Personen bestimmte Zugriffsarten durchführen bzw. nicht durchführen dürfen.

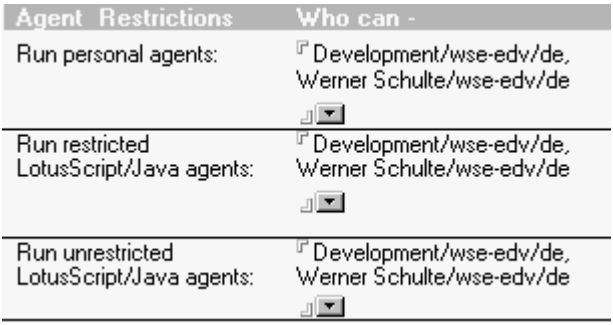
Server Access	Who can -
Only allow server access to users listed in this Directory:	No
Access server:	
Not access server:	
Create new databases:	
Create replica databases:	Werner Schulte/wse-edv/de, Development/wse-edv/de
Allowed to use monitors:	*
Not allowed to use monitors:	
Administer the server from a browser:	Development/wse-edv/de, Werner Schulte/wse-edv/de

Serverzugriff

- Nur Personen des Domino-Verzeichnisses dürfen auf den Server zugreifen (Nein: keine Einschränkung).
- Einzelne Personen oder Gruppen dürfen zugreifen (kein Eintrag: keine Einschränkung).
- Einzelne Personen oder Gruppen dürfen nicht zugreifen (kein Eintrag: keine Einschränkung).
- Einzelne Personen oder Gruppen dürfen neue Datenbanken auf dem Server anlegen (kein Eintrag: keine Einschränkung).
- Einzelne Personen oder Gruppen dürfen Repliken auf dem Server anlegen (kein Eintrag: Niemand darf Repliken anlegen!)
- Überwachung benutzen („*“: keine Einschränkung)

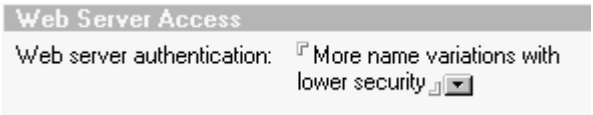
- Keine Überwachung benutzen (kein Eintrag: keine Einschränkung).
- Den Server über einen Browser verwalten (kein Eintrag: Administratoren haben Zugriff über Browser).

Agenten sind als vielseitige Helfer ein Teil des Domino-Systems. Sollen solche Programme auf dem Server gestartet werden, so muss im Abschnitt „Agent-Beschränkungen" geregelt werden, wer das Recht dazu haben soll.



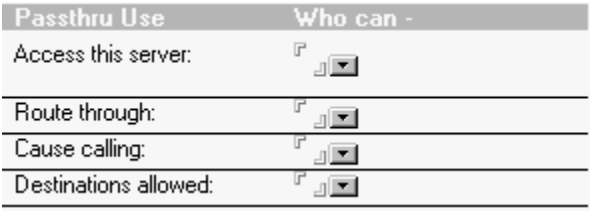
Agent-Beschränkungen

Wer in diesen Feldern nicht als Person oder Gruppe eingetragen ist, kann keine Agenten auf dem Server starten. Als Person gilt dabei derjenige, der den Agenten signiert (erstellt oder zuletzt geändert) hat.



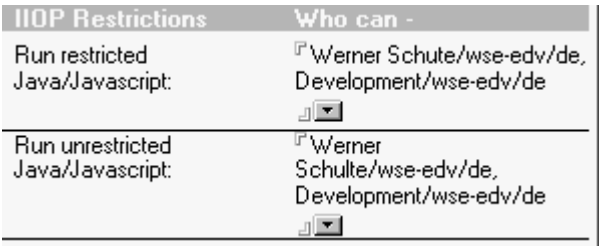
Web-Server-Zugriff

Das Feld „Web-Server-Zugriff“ erlaubt die Beschränkung der Namenseingabe in Browsern auf die Notes-Syntax mit hierarchischen Namensbestandteilen (z. B. Perter Muster/WSE3/de).



Benutzung des Durchgangs-Servers

Der Abschnitt „Benutzung des Durchgangs-Servers“ definiert Server, Personen oder Gruppen, die den Server als Durchgangs-Server in verschiedenen Stufen verwenden dürfen. Ist hier nichts eingetragen, kann der Server nicht als Durchgangs-Server eingesetzt werden.



Ausführung von Java-Applets oder Javascript

Der Abschnitt „Internet Inter-ORB-Protokoll-Beschränkungen“ enthält Einträge für die Erlaubnis Java-Applets bzw. Javascript-Funktionenen auf dem Server auszuführen.

9.1.2 Sicherheit auf der Ebene der Datenbank und der Masken

Die erste Stufe der Zugriffskontrolle auf Datenbanken stellt die Zugriffskontrollliste dar. Über Zugriffsebenen, Benutzertyp und einzelne Zugriffsberechtigungen wird hier geregelt, welcher Benutzer, welcher Server und welche Gruppe auf die verschiedenen Datenbankelemente zugreifen können. Der Zugriff kann zusätzlich über Verschlüsselung und elektronische Signaturen erschwert werden.

Im Rahmen der Datenbankgestaltung kann der Entwickler für einen differenzierten Zugriff auf die einzelnen Elemente der Datenbank sorgen. Ansichten und Masken können sowohl bei den Lese- als auch bei den Autorenrechten eingeschränkt werden. In Masken können Lese- und Autorenrechte vergeben und auch während der Benutzung automatisch verändert werden. Über verborgene Felder und Abschnitte in Masken kann der Zugang zu Informationen auf bestimmte Benutzer bzw. Benutzergruppen reduziert werden. Sogar einzelne Felder können verschlüsselt werden.

9.1.2.1 Die Zugriffskontrollliste

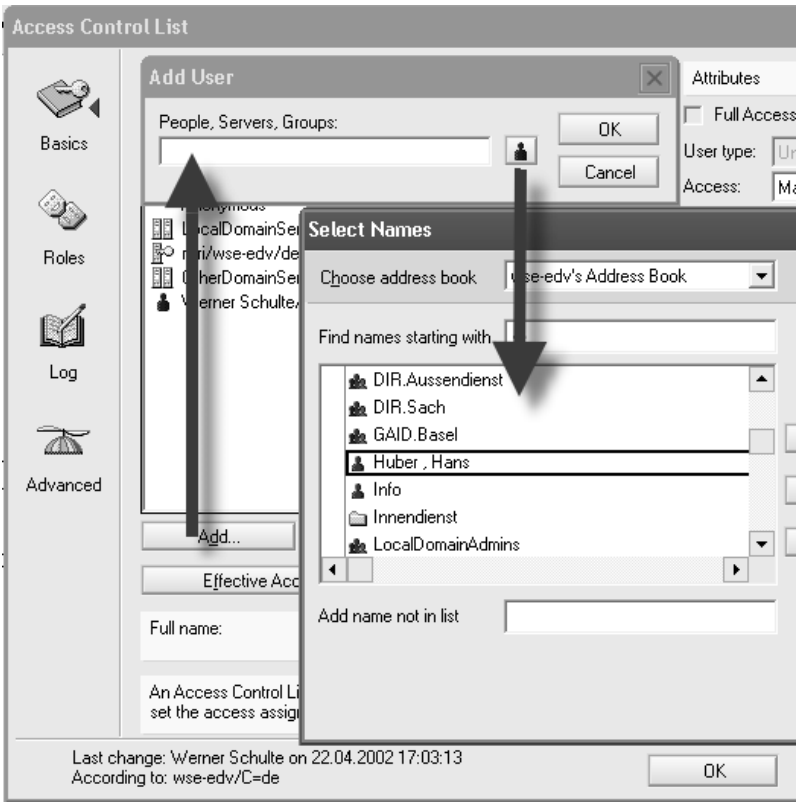
Die Zugriffskontrollliste einer Datenbank ist das wichtigste Sicherheitselement, das Notes und Domino verwenden, um die Daten vor unbefugtem Zugriff zu schützen. Dieser Schutz wird unterschiedlich wirksam – je nachdem, ob die Datenbank auf einem Server oder einer Arbeitsstation gespeichert ist. Die Zugriffskontrollliste regelt, wer und mit welchen Rechten Daten

einer Datenbank lesen oder bearbeiten kann. Dazu kommen die Rechte zur Verwaltung der Datenbank selbst. Die Bearbeitung der Zugriffskontrollliste erfolgt bei einer einzelnen Datenbank über den Notes-Client im Menü „Datei / Datenbank / Zugriffskontrollliste“. Im Register „Allgemein“ werden die wichtigsten Einstellungen zu den Zugriffsrechten auf die Datenbank vorgenommen.

Zugriffskontrollliste bearbeiten

Im Register „Allgemein“ werden die Rechte für Personen, Gruppen und Server festgelegt. Es können alle Personen oder eine Personenauswahl mit Rechten an der Datenbank angezeigt werden. In der Benutzerliste sind zu finden:

- **Personen**
  Hier werden Personen mit ihrem qualifizierten oder alternativen Namen aufgeführt. Eine Auswahl ist möglich, wenn die Schaltfläche „Hinzufügen“ verwendet wird.

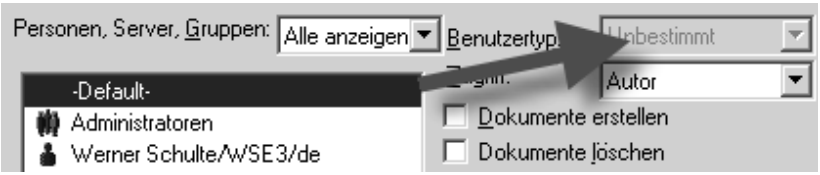


Personen in der Zugriffskontrollliste

- **Server**
  Server können einzeln oder über Gruppen in der Zugriffskontrollliste aufgeführt sein.

- **Gruppen**
  Bei den Gruppen werden zwischen Personen-Gruppen, Server-Gruppen und gemischten Gruppen unterschieden.
  Standardmäßig sind die Server-Gruppen „LocalDomainServers“ und „OtherDomainServers“ verfügbar. Die Gruppe „LocalDomainServers“ erhält in diesem Fall Manager-Rechte. Sie sollte mindestens „Entwickler“-Rechte besitzen, damit die Datenbank repliziert werden kann.

- **Standard**
  Als Standardbenutzer wird derjenige Benutzer oder Server aufgefasst, der in keiner der übrigen Definitionen der Zugriffskontrollliste einer Datenbank enthalten ist. Dem Standardbenutzer ist kein Benutzertyp zugeordnet. Die Rechte-Stufe dieses Benutzers wird in der Regel nicht sehr hoch angesiedelt sein (also z.B. „Leser“), weil die Datenbank sonst nicht gerade sicher ist.



Benutzertyp des Standardbenutzers

Häufig wird der Standardbenutzer ganz aus der Verwendung einer Datenbank ausgeschlossen. Dann ist es sehr wichtig, alle Benutzer, die Zugriff auf die Datenbank haben sollen, als Mitglied einer Gruppe oder einzeln in der Benutzerliste der Datenbank aufzuführen.

- **Anonymus**
  Ein weiterer spezieller Benutzer trägt den Namen "Anonymus". Dieser Benutzer wurde im Rahmen des Web-Zugriffes eingeführt und entspricht allen den Benutzern, die im Sinne von Notes und Domino nicht definiert sind, zu denen also keine Benutzerinformationen in einem Verzeichnis gefunden wurden.

- **Platzhalter**
  Um die Mitglieder einer Unterorganisation gemeinsam in der Benutzerliste zu verwenden, können Platzhalter eingesetzt werden. Ein solcher Eintrag kann also z.B. lauten: */Marketing/wse-edv/de.

Bei einer neuen Datenbank werden automatisch die Benutzer „Standard", „LocalDomainServers", „OtherDomainServers" sowie der „Ersteller der Datenbank" in die Benutzerliste der Zugriffskontrollliste aufgenommen.

Wenn ein Benutzer in mehreren Einträgen enthalten ist (z.B. in Gruppen und direkt), gelten folgende Regeln:

- Ist ein Benutzer direkt oder über eine Gruppe mit dem Recht „Kein Zugriff" verbunden, gilt das vorrangig.

- Ist ein Benutzer Mitglied in mehreren aufgeführten Gruppen, gilt das Recht der Gruppe mit der höchsten Rechte-Stufe.

- Ist ein Benutzer direkt und als Mitglied einer Gruppe eingetragen, so gilt die Rechte-Definition des direkten Eintrags.

Jedem Eintrag in der Benutzerliste werden ein Benutzertyp, eine Rechte-Stufe, spezielle Rechte und eventuell Funktionen zugeordnet.

9.1.2.1.1 Benutzertypen

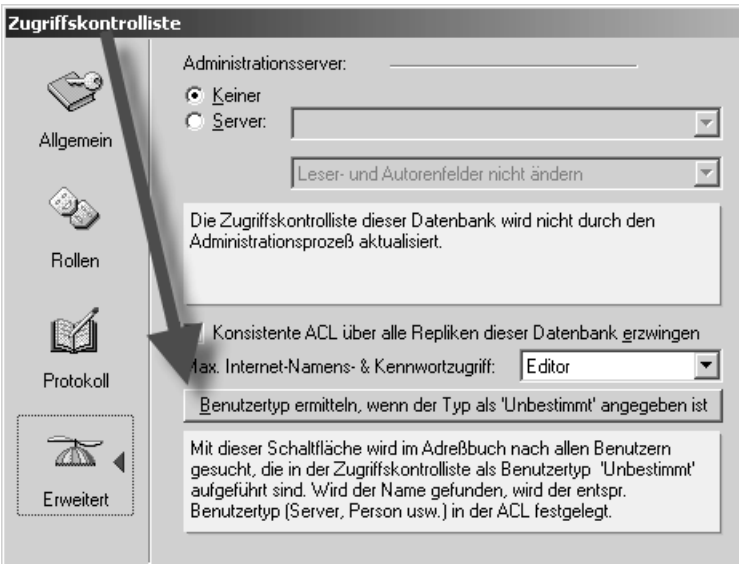
Das Feld „Benutzertyp“ nimmt die erste grobe Einteilung der Benutzer in Bezug auf ihre Rechte vor. Dabei wird zwischen Personen, Servern und Gruppen unterschieden. Ein Benutzer vom Typ „Server“ kann nicht über den Notes-Client auf eine Datenbank zugreifen. Deshalb ist es so wichtig, generell Benutzertypen zu vergeben. Für den Benutzertyp sind folgende Auswahlmöglichkeiten gegeben:

- Person
- Server
- Gemischte Gruppe
- Personengruppe
- Servergruppe
- undefiniert

Der Benutzer „Standard“ hat immer den Benutzertyp „undefiniert“.

Achtung!

Wurden in der Zugriffskontrollliste einer Datenbank Benutzer hinzugefügt, ohne ihnen einen Benutzertyp zuzuweisen, so kann das auf einfache Weise nachgeholt werden. In dem Register „Erweitert“ befindet sich eine Schaltfläche „Benutzertyp ermitteln“.



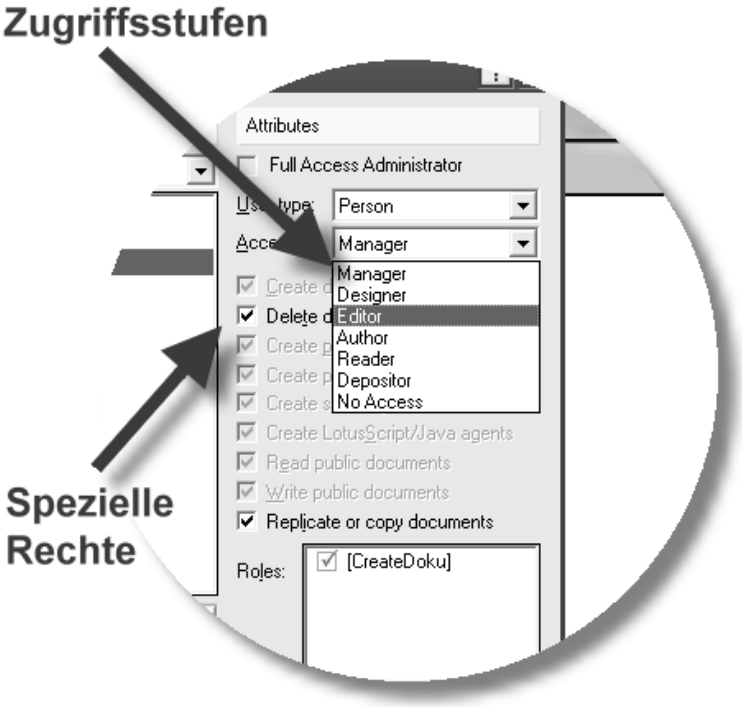
Benutzertyp ermitteln

Wird sie verwendet, so ermittelt der Client aus dem Domino-Verzeichnis den Typ. Personen und Server werden als solche eingetragen. Gruppen werden grundsätzlich als „gemischte Gruppe“ eingetragen.

Gemischte Gruppen können sowohl Personen als auch Server enthalten.

9.1.2.1.2 Zugriffsstufen

Über die Zugriffsstufen wird den verschiedenen Benutzern und Servern erlaubt, in einem vordefinierten Rahmen auf eine Datenbank zuzugreifen. Es wird auf einfache Art geregelt, welche Rechte der Benutzer haben soll. Da diese Vorgehensweise nicht jeder Situation gerecht wird, bietet die Zugriffskontrollliste die Möglichkeit, die erteilten Rechte, noch einmal einzeln zu differenzieren.



Zugriffsstufen und einzelne Rechte

Für die Rechte einer Benutzerstufe gilt grundsätzlich, dass sie alle Rechte der niedrigeren Benutzertypen beinhaltet. Es ergibt sich eine Rechte-Hierarchie mit folgenden Stufen:

- **Kein Zugriff**
  Ein Benutzer oder Server, dem dieser Benutzertyp zugeordnet wird, hat keinerlei Rechte an einer Datenbank und deren Daten. Die einzige Ausnahme stellen Dokumente in der Datenbank dar, deren Maske die Eigenschaft „Verfügbar für Benutzer mit öffentlichem Zugriff" haben. Diese Eigenschaft wird bei der Erstellung der Maske im Designer-Client festgelegt. In der Zugriffskontrollliste kann bestimmt werden, ob diese Benutzer öffentliche Dokumente lesen oder ändern und ob sie Dokumente replizieren oder kopieren dürfen.

- **Einlieferer**
  Für Einlieferer ist nur das Erstellen von Dokumenten möglich. Weder kann er Änderungen durchführen noch darf er Dokumente lesen. Öffentliche Dokumente darf er bearbeiten, wenn diese Rechte nicht einzeln entfernt wurden. Das Gleiche gilt für das Kopieren und Replizieren von Dokumenten. Diese Zugriffsstufe wird vorwiegend für Archivierungsaufgaben eingesetzt.

- **Leser**
  Der Leser kann Dokumente nur anzeigen, also keine Dokumente erstellen oder ändern. Öffentliche Dokumente können geändert werden und das Kopieren und Replizieren von Dokumenten kann erlaubt werden. Das Leserecht ist fest mit der Zugriffsstufe verbunden.

- **Autor**
  Der Autor kann, soweit dieses Recht nicht entfernt wurde, Dokumente erstellen und diese lesen. Ein Autor kann Dokumente nur dann ändern, wenn das Dokument ein Autorenfeld enthält, in dem der Name dieses Benutzers aufgeführt ist. Das gilt auch für Dokumente, die der Benutzer selbst erstellt hat.

- **Editor**
  Im Gegensatz zum Autoren kann ein Editor sowohl eigene als auch fremde Dokumente ändern. Er kann Dokumente erstellen und natürlich auch lesen.

- **Entwickler**
  Zusätzlich zu den Funktionen der niedrigeren Zugriffsstufen kann der Entwickler Gestaltungselemente bearbeiten. Bis auf die Möglichkeiten, Dokumente zu löschen, Agenten zu erstellen und Dokumente zu replizieren, sind alle Rechte fixiert und können nicht abgewählt werden.

- **Manager**
  Neben den Standardrechten kann der Manager die Datenbank selbst löschen, die Zugriffskontrollliste verwalten und die Datenbank verschlüsseln.

9.1.2.1.3 Spezielle Rechte

Je nach verwendeter Zugriffsstufe sind unterschiedliche Rechte hinzufügbar oder abwählbar. Damit wird eine genaue Rechte-Definition für Ausnahmefälle möglich. Einige der Rechte sind fest mit der Zugriffsstufe verbunden (grau hinterlegt) und nicht veränderbar. Andere sind offen und können mit einem Häkchen

versehen bzw. leer gelassen werden. Für die verschiedenen Zugriffsstufen erhält man folgendes Bild:

Für die Zugriffsstufe „Designer“ (und damit auch für Manager) gilt, dass zusätzlich Gestaltungselemente der Datenbank bearbeitet werden können. Dieses Recht ist nicht abwählbar.

Persönliche Agenten können nur von dem Ersteller, Entwickler und Manager verwendet werden. Sie können auf Arbeitsstationen und Servern ausgeführt werden. In beiden Fällen sind zusätzliche Einstellungen notwendig.

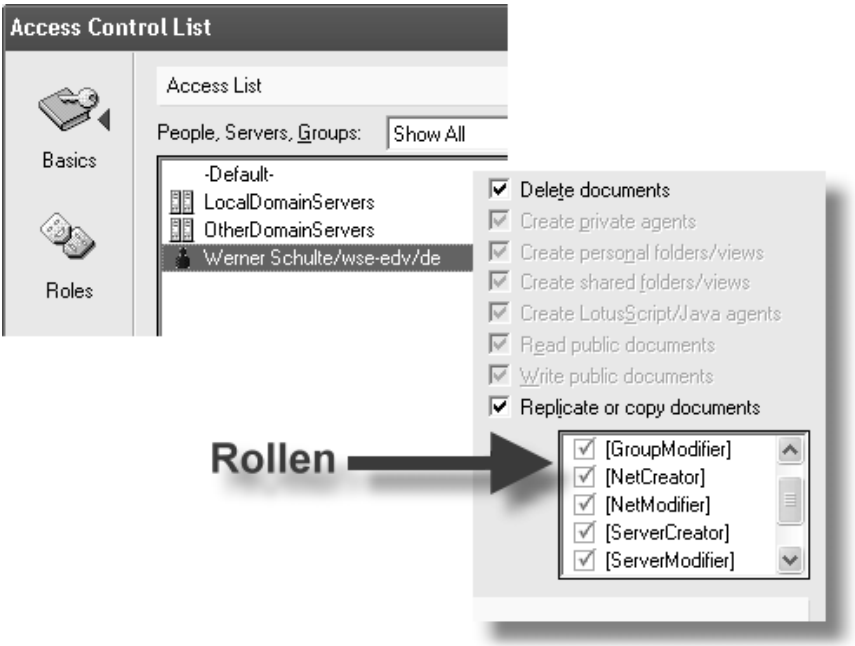
Persönliche Ordner und Ansichten können zwar bei einigen Zugriffsstufen deaktiviert, aber nicht verhindert werden. Ist das Recht zur Erstellung persönlicher Ordner und Ansichten nicht erlaubt, dann werden sie für diese Benutzer auf dessen Arbeitsstation gespeichert. Dadurch wird die Datenbank selbst von zusätzlichen Indizes und Verweistabellen entlastet.

	kein Zugriff	Einleferer	Leser	Autor	Editor	Entwickler	Manager
Dokument erstellen	nein	ja	nein	mög-lich	ja	ja	ja
Dokument lesen	nein	nein	ja	ja	ja	ja	ja
Dokument schreiben	nein	nein	nein	ja	ja	ja	ja
Dokument löschen	nein	nein	nein	mög-lich	mög-lich	mög-lich	mög-lich
Persönl. Agenten erstellen	nein	nein	mög-lich	mög-lich	mög-lich	ja	ja
Persönl. Ordner / Ansichten erstellen	nein	nein	mög-lich	mög-lich	mög-lich	ja	ja
Gemein-same Ordner / Ansichten erstellen	nein	nein	nein	nein	mög-lich	ja	ja
Lotus-Script / Java-Agenten erstellen	nein	nein	mög-lich	mög-lich	mög-lich	mög-lich	ja
öffentl. Dokument lesen	mög-lich	mög-lich	ja	ja	ja	ja	ja
öffentl. Dokument schreiben	mög-lich	mög-lich	mög-lich	mög-lich	ja	ja	ja
Dokument replizieren oder kopieren	mög-lich	ja	mög-lich	mög-lich	mög-lich	mög-lich	mög-lich

Rechte-Tabelle

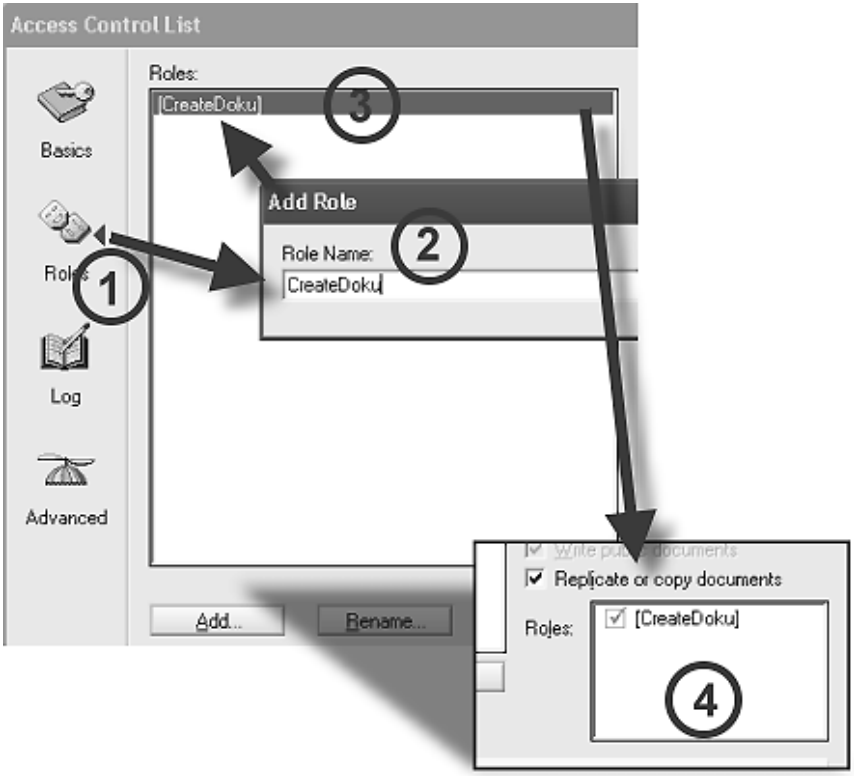
9.1.2.1.4 Rollen

Rollen stellen eine weitere Form der Rechte-Differenzierung dar. Zunächst bieten sich die Rollen wie normale Rechte an. Sie können einem Benutzer oder einem Server zugewiesen werden. Der Unterschied zu den normalen Rechten besteht darin, dass Rollen vom Entwickler in seinen Anwendungen ganz gezielt eingesetzt werden können. Es hängt also an einer Rolle kein direkt erkennbares Recht. Die genaue Wirkung wird dem Benutzer erst zur Laufzeit der Anwendung zugewiesen.



Rollen

Die Definition der Rollen wird entsprechend der Funktion durch den Anwendungsentwickler vorgenommen.



Rolle erstellen

Die Rolle wirkt zwar nur, wenn im Programm eine Verwendung vorgesehen ist. Sie kann aber unabhängig davon angelegt und entfernt werden. Es ist also z.B. möglich, Rollen in der Datenbankanwendung vorzusehen, sie aber erst später zu aktivieren.

❶❷❸ Ausführungsschritte:

1. Register „Rollen“ in der Zugriffskontrollliste auswählen.

2. Über die Schaltfläche „Anlegen“ das entsprechende Dialogfenster öffnen und den Namen der neuen Rolle anlegen (der Name muss exakt dem im Programm verwendeten entsprechen!).

3. Nachdem die Rolle in der Liste der verfügbaren Rollen erscheint, zurückgehen zum Register „Allgemein“.

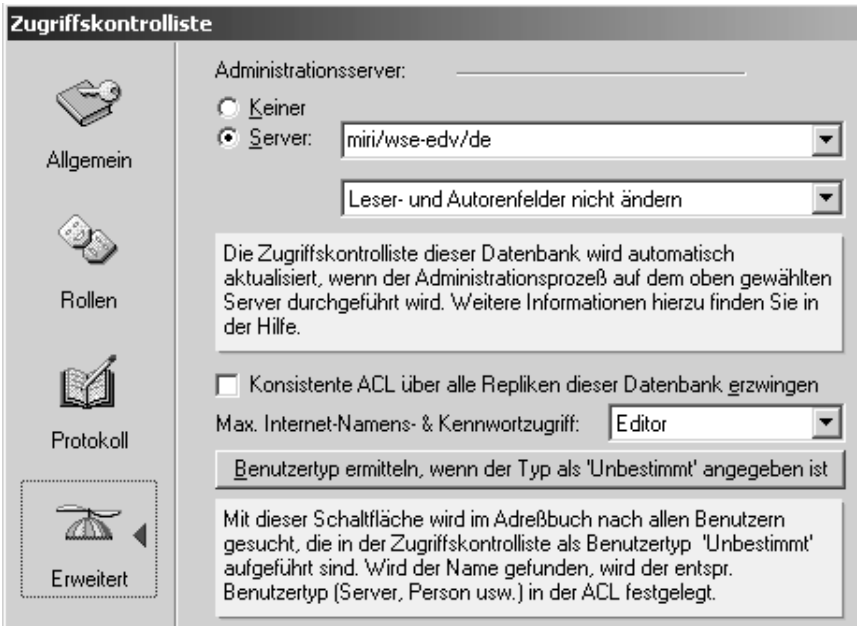
4. Die neue Rolle ist jetzt im Fenster „Rollen“ aufgeführt und kann bei den Benutzern aktiviert werden, die das im Programm hinterlegte Recht ausüben sollen.

❶❷❸

Die Rollen können natürlich nur solche Aktionen steuern bzw. zulassen, die mit der Zugriffsstufe des Benutzers oder Servers auch erlaubt sind.

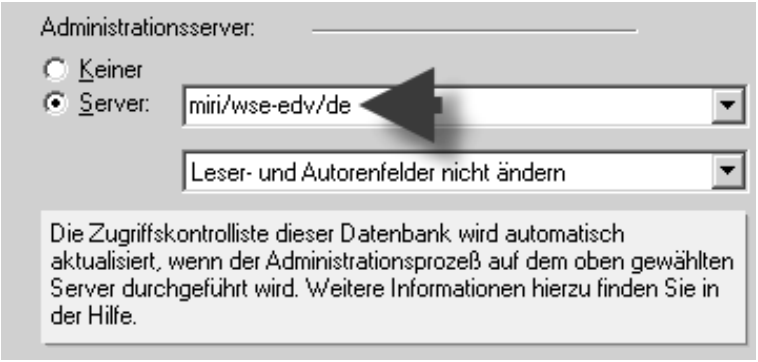
9.1.2.1.5 Erweiterte Einstellungen

Im Register „Erweitert“ sind einige Funktionen zusammengefasst, die auch den Namen „Sonstiges“ führen könnten. Es handelt sich um zusätzliche Werkzeuge und Einstellungen.



Die erweiterte Zugriffskontrollliste

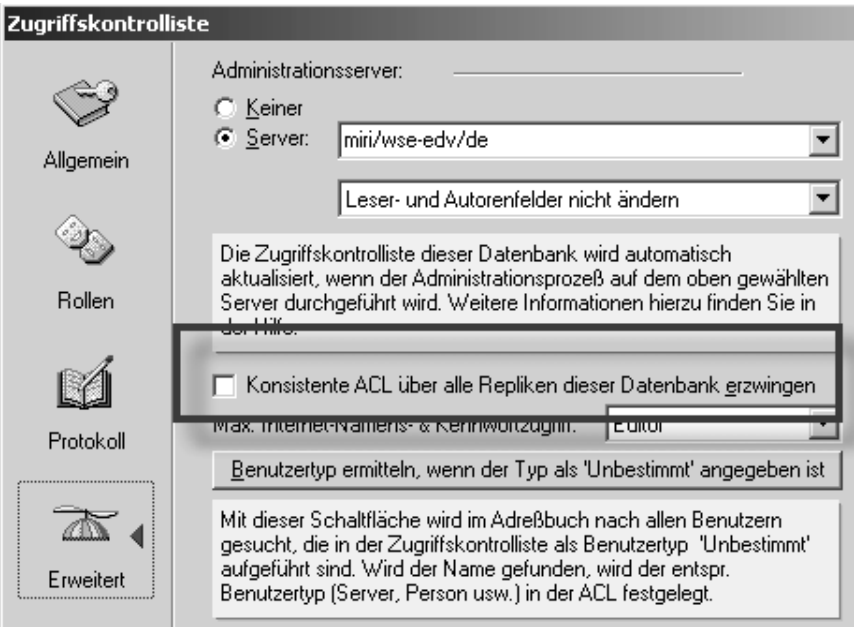
Die erste Angabe dient der Definition eines Administrationsservers. Die wichtigste Funktion des Administrationsprozesses besteht für die Datenbanken darin, dass Änderungen im Dominoverzeichnis zu Personen und Gruppen in der Zugriffskontrollliste nachgeführt werden.



Administratorserver

Ist z.B. eine Person ausgeschieden und im Dominoverzeichnis gelöscht, so sorgt ein Administrationsprozess dafür, dass dieser Benutzer aus den Zugriffskontrolllisten gelöscht wird, in denen dieser Benutzer aufgeführt war.

Eine wichtige Sicherheitsfunktion ist mit einem einfachen Anhaken zu aktivieren: „Konsistente ACL über alle Repliken dieser Datenbank erzwingen“. Diese Funktion ist deshalb vorhanden, weil normalerweise die Wirkung der Zugriffskontrollliste auf den Domino-Server beschränkt ist.



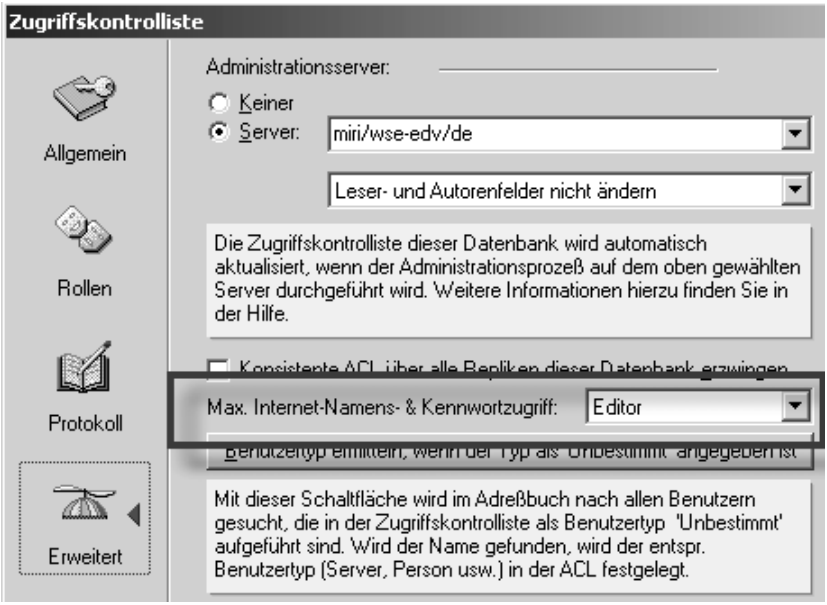
Konsistente Zugriffskontrollliste

Der Notes-Client (sowohl auf der Arbeitsstation als auch auf dem Server-Rechner) wird durch die Zugriffskontrollliste zunächst nicht beeinflusst und gibt seinem Benutzer Managerrechte, wenn er lokal (also nicht über einen Server-Prozess) auf eine Datenbank zugreift. Die Aktivierung der konsistenten ACL sorgt dafür,

dass wirklich nur noch Benutzer mit Managerrechten die Zugriffskontrollliste verändern dürfen.

Bei der Aktivierung der konsistenten Zugriffskontrollliste ist es sehr wichtig, darauf zu achten, dass genügend Personen mit Managerrechten in der Benutzerliste der Zugriffskontrollliste aufgeführt sind. Ist das nicht der Fall, kann es dazu kommen, dass die Zugriffskontrollliste einer Datenbank nicht mehr geändert werden kann.

Das Feld „Maximalen Internetzugriff festlegen“ erlaubt es, den Datenbankzugriff von Benutzern einzuschränken, die über das Internet auf eine Datenbank zugreifen und sich mit Name und Kennwort ausweisen.



Maximaler Zugriff über das Internet

Es können dabei alle oben aufgeführten Zugriffsstufen aus einer Liste ausgewählt werden. Ein Benutzer, der sich nicht ausweist, wird als Standardbenutzer mit dem Benutzernamen „Anonymus“ behandelt. Es empfiehlt sich, einen solchen Benutzer anzulegen, wenn eine Datenbank über das Internet verfügbar ist. Wenn nur Domino- und Notes-Benutzer auf eine solche Datenbank zugreifen, ist es sinnvoll, dem Benutzer „Anonymus“ die Zugriffsstufe „Kein Zugriff“ zu geben.

9.1.2.1.6 Das Protokoll der Zugriffskontrollliste

Jede Änderung der Zugriffskontrollliste wird in der Datenbank gespeichert und kann über das Register „Protokoll“ angezeigt werden:

Change history:

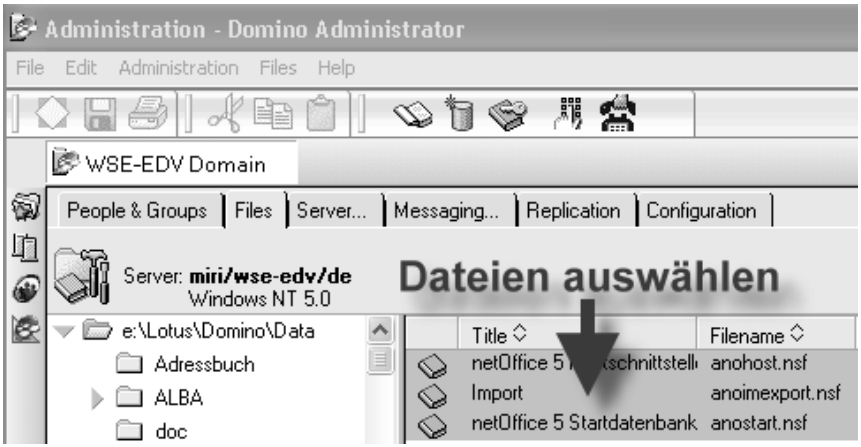
Date/Time	Action
22.10.2000 21:26:40 Werne	Schulte/wse-edv/de aktualisierte Administratoren
22.10.2000 21:26:32 Werne	Schulte/wse-edv/de fügte Administratoren hinzu
13.10.99 17:00:31 Werner	Schulte/WSE3/de aktualisierte Werner Schulte/wse-edv
13.10.99 17:00:20 Werner	Schulte/WSE3/de fügte Werner Schulte/wse-edv/de hir
10.10.99 15:41:10 Werner	Schulte/WSE3/de updated WSE Development/WSE3/c
10.10.99 15:41:05 Werner	Schulte/WSE3/de added WSE Development/WSE3/de
10.10.99 15:40:57 Werner	Schulte/WSE3/de updated Werner Schulte/WSE3/de
10.10.99 15:40:52 Werner	Schulte/WSE3/de updated -Default-
10.10.99 15:40:14 Werner	Schulte/WSE3/de updated Werner Schulte/WSE3/de
10.10.99 15:40:14 Werner	Schulte/WSE3/de updated role [CreateDoku]
10.10.99 15:40:14 Werner	Schulte/WSE3/de added Werner Schulte/WSE3/de

Zugriffsprotokoll einer Datenbank

Es werden in diesem Protokoll lediglich das Datum, die Uhrzeit, der Benutzer und die Art der Änderung angezeigt.

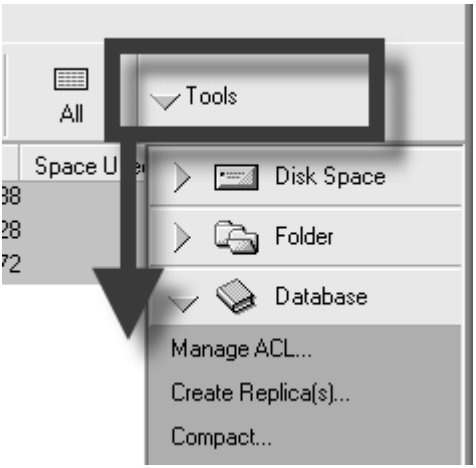
9.1.2.1.7 Zugriffskontrolllisten im Administrator-Client

Eine erweiterte Form der Verwaltung von Zugriffskontrolllisten stellt der Administrator-Client zur Verfügung.



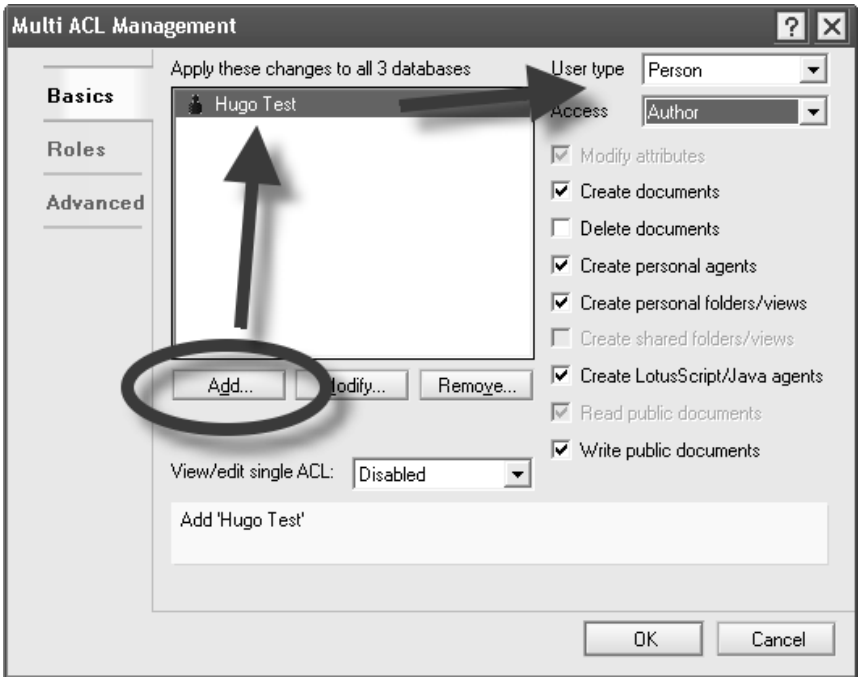
Mehrere Datenbanken im Administrator-Client bearbeiten

Im Register „Dateien“ werden die gewünschten Datenbanken markiert und unter „Werkzeuge / Datenbanken“ die Position „Zugriffskontrollliste bearbeiten“ ausgewählt.



Die Position „Zugriffskontrollliste bearbeiten“

In der dann folgenden Dialogbox können direkt bestimmte Aktionen für mehrere Datenbanken vorgenommen werden (z.B. eine Person zur Zugriffskontrollliste hinzufügen). Die Angaben, die hier gemacht werden, trägt der Administrator-Client in die Zugriffskontrolllisten der markierten Datenbanken ein.



Eintrag zur Zugriffskontrollliste hinzufügen

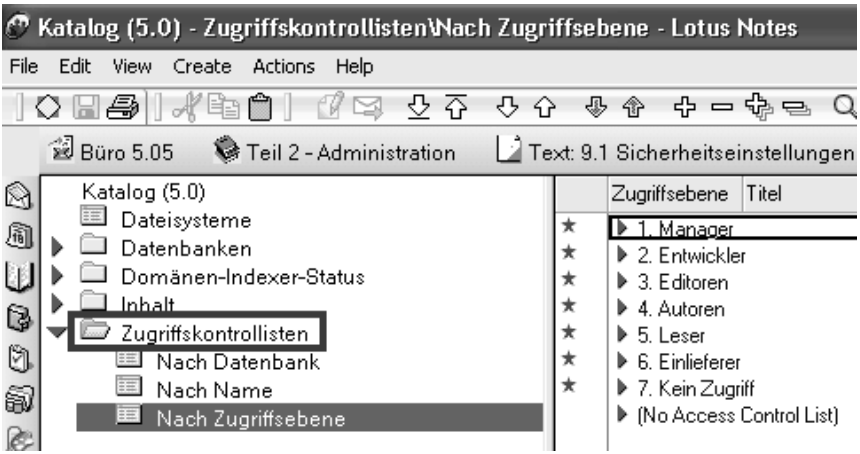
Änderungen sind nur bei den einzelnen Datenbanken möglich. Dazu kann in der Dialogbox - in der Liste „Einzeln anzeigen / bearbeiten“ - jede der vorgewählten Datenbanken angeklickt und bearbeitet werden. Die Bearbeitung der Zugriffskontrollliste ent-

spricht dann je Datenbank der Vorgehensweise über das Menü „Datei / Datenbank / Zugriffskontrollliste“.

9.1.2.1.8 Zugriffskontrolllisten im Datenbankkatalog

Zur Analyse und zum schnelleren Überblick können die Zugriffskontrolllisten als Ansichten im Datenbankkatalog angezeigt werden. Es sind drei Ansichten verfügbar, die nach Zugriffseigenschaften sortiert sind:

- nach Datenbanken
- nach Name
- nach Zugriffsebene



Ansichten des Datenbankkatalogs

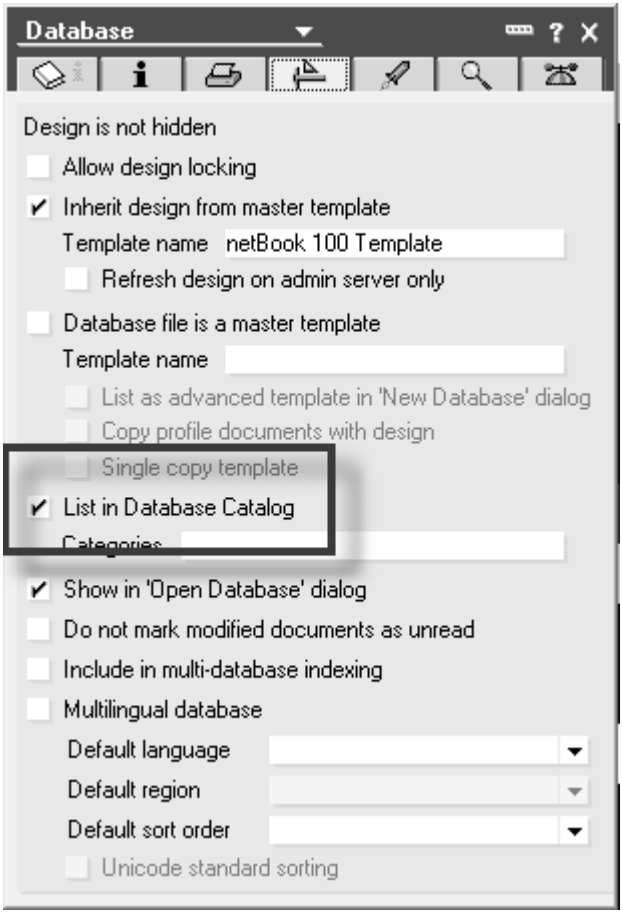
Zu jeder Datenbank ist im Datenbankkatalog ein Dokument enthalten, das neben anderen Informationen auch eine Übersicht der Zugriffsrechte auf die Datenbank enthält.

		Zugriffskontrolliste				
		Aktionen				
	Namen	CrDoc	DlDoc	PerAg	PerFld	ShrFld
Manager:	Administratoren	1	1	1	1	1
	Info/wse-edv/de	1	1	0	0	0
	LocalDomainServers	1	1	1	1	1
	miri/wse-edv/de	1	1	0	0	0
	Werner Schulte/wse-edv/de	1	1	1	1	1
Entwickler:						
Editoren:						
Autoren:						
Leser:						
Einlieferer:						
Kein Zugriff:	-Default-	0	0	0	0	0
	OtherDomainServers	0	0	0	0	0
	Anonymous	0	0	0	0	0

Verwendete Abkürzungen:
CrDoc = Dokumente erstellen
DlDoc = Dokumente löschen
PerAg = persönliche Agenten erstellen
PerFld = persönliche Ordner/Ansichten erstellen
ShrFld = gemeinsame Ordner/Ansichten erstellen
LscAg = LotusScript/Java Agenten erstellen
RdPub = öffentliche Dokumente lesen
WrPub = öffentliche Dokumente schreiben

Zugriffsrechte im Datenbankkatalog

Im Datenbankkatalog sind allerdings nur solche Datenbanken aufgeführt, in deren Eigenschaften das Feld „Im Datenbankkatalog auflisten“ aktiviert ist.



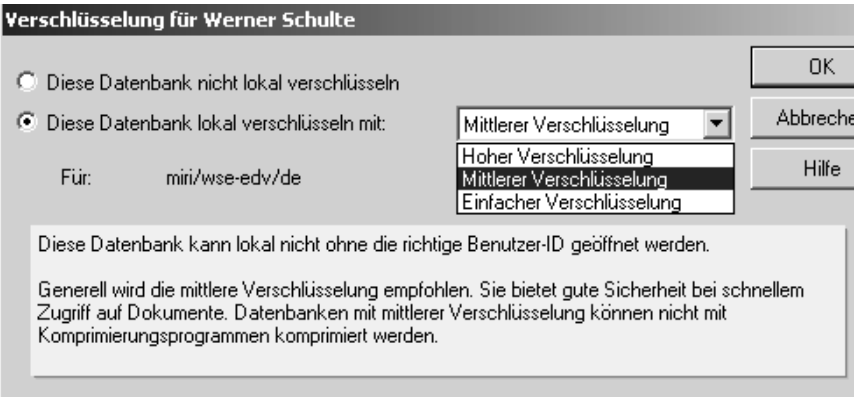
Datenbankeigenschaften

Eine Bearbeitung der Zugriffskontrollliste über den Datenbankkatalog ist nicht möglich.

9.1.2.2 Verschlüsselung lokaler Datenbanken

Datenbanken, die auf einer lokalen Arbeitsstation gespeichert sind, können leichter in falsche Hände geraten als solche, die sich auf Servern (also in der Regel in speziell gesicherten Räumen) befinden. Besonders gefährdet sind Datenbanken auf mobilen Arbeitsstationen. Als Instrument der Sicherung solcher Daten kann die Verschlüsselung der Datenbank eingesetzt werden. Bei dieser Vorgehensweise wird die komplette Datenbank verschlüsselt und ist nur noch von solchen Benutzern zu öffnen, die über den entsprechenden Schlüssel verfügen.

Soll eine Datenbank verschlüsselt werden, so ist das über die Datenbankeigenschaften möglich. Voraussetzung ist allerdings, dass der Benutzer, der die Verschlüsselung durchführt, über Managerrechte an der Datenbank verfügt.



Datenbankverschlüsselung

Die Verschlüsselungsstufen bestimmen, wie leicht und wie schwer der Text in der Datenbank wieder entschlüsselt werden kann. Grundsätzlich gilt, je höher der Verschlüsselungsgrad, desto schwieriger ist die Entschlüsselung und entsprechend gut ist auch die Datenbank geschützt. Bei einer hohen Verschlüsselung erhöht sich allerdings auch die Dauer für das Schreiben und Lesen von Datenbankdokumenten. Es empfiehlt sich in der Regel die mittlere Verschlüsselung zu wählen. Dieser Wert wird deshalb auch standardmäßig vorgeschlagen.

9.1.2.3 Zugriffsrechte auf Ansichten

Ansichten stellen Gestaltungselemente dar, denen der Entwickler auch Eigenschaften in Bezug auf ihre Nutzungsrechte mitgeben kann. Die Rechte an der Nutzung einer Ansicht sind in einem eigenen Register einstellbar.

Ansichtsrechte

Die Standardeinstellung besagt, dass alle Benutzer mit Leserecht oder höherer Zugriffsstufe eine Ansicht verwenden dürfen. Wird diese Grundeinstellung deaktiviert, kann in der darunter stehenden Liste angehakt werden, wer die Ansicht einsetzen darf.

Der Zugriffsschutz einer Ansicht hat keine Auswirkung auf die angezeigten Dokumente. Die Dokumente sind also im Zweifel über andere Ansichten verfügbar. Wenn der Benutzer persönliche Ansichten erstellen darf, ist er auch in der Lage eine Ansicht zu erstellen, die die gleichen Eigenschaften aufweist wie die geschützte Ansicht.

Sind Benutzer oder Benutzergruppen zum Lesen oder Bearbeiten von öffentlichen Dokumenten zugelassen, so kann in der Ansicht aktiviert werden, dass solche Benutzer keinen Zugriff auf die Ansicht haben.

9.1.2.4 Zugriffsrechte auf Masken, Abschnitte und Felder

Einzelne Dokumente und Dokumentteile können über Schutzmechanismen sicherer gemacht werden, die in der Maske in unterschiedlicher Form vom Entwickler hinterlegt werden. Ähnlich den Ansichten verfügen auch die Masken über Eigenschaften, die den Zugriffsschutz für die Dokumente regeln, die mit ihnen erstellt wurden.

Zugriffsrechte auf Dokumente über eine Maske

Zusätzlich zur Lesebeschränkung wird hier auch die Schreibbeschränkung ermöglicht. Damit ein Dokument nicht kopiert, als

e-Mail versendet oder gedruckt werden kann, ist hier eine spezielle Eigenschaft aktivierbar.

Weitere Sicherheit können spezielle Felder in den Dokumenten bieten. Da Felder nur im Design-Modus erstellt werden können, müssen sie vom Entwickler bereits vorgesehen werden. Für die Steuerung von Personenabhängigkeiten bietet Notes spezielle Feldtypen:

- **Namensfelder**
  unterstützen die hierarchischen Namen von Notes und Domino, sind aber nicht zur Steuerung von Rechten verwendbar.

- **Leserfelder**
  können die Rechte zum Lesen von Dokumenten auf solche Benutzer beschränken, die darin aufgeführt sind. Diese Benutzer müssen mindestens die Zugriffsstufe „Leser“ besitzen.

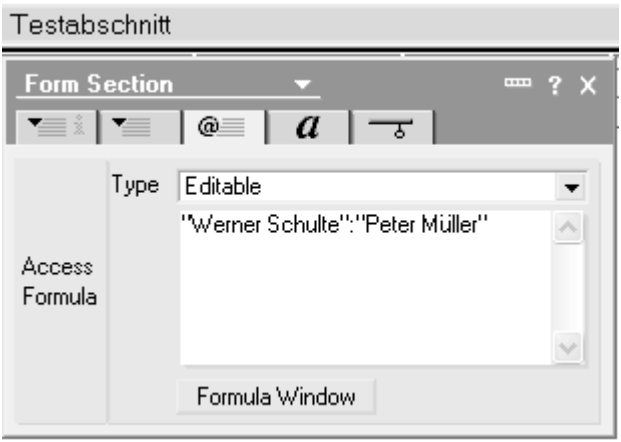
Wenn ein Leserfeld in einem Dokument enthalten ist, dürfen es nur Benutzer sehen, die in einem Leserfeld des Dokumentes aufgeführt sind. Damit solche Dokumente repliziert werden können, müssen die Server ebenfalls im Leserfeld erscheinen.

- Autorenfelder
  Benutzer, die über die Zugriffsstufe „Autor“ verfügen und in einem solchen Feld aufgeführt sind, dürfen das Dokument bearbeiten.

Achtung!

Auch solche Autoren, die ein Dokument erstellt haben, können es nicht bearbeiten, wenn sie nicht in einem Autorenfeld dieses Dokuments enthalten sind. Deshalb sollte jede Maske normalerweise ein Autorenfeld beinhalten, in das der Ersteller des Dokuments eingetragen wird.

Die nächste Ebene, auf der eine Beschränkung der Zugriffsrechte erfolgen kann, ist der Abschnitt innerhalb eines Dokuments. Der Entwickler der Datenbank kann für den Abschnitt eine Formel hinterlegen, deren Ergebnis steuert, welche Benutzer mit diesem Abschnitt arbeiten dürfen.



Berechtigungsformel eines Abschnitts

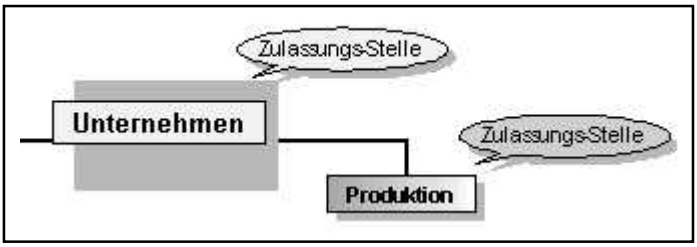
Ob die Benutzer Felder in diesem Abschnitt editieren dürfen, wird ebenfalls bei den Eigenschaften des Abschnitts im Entwurfsmodus festgelegt.

Diese Seite ist zur Zeit nicht belegt.

9.2 Das Konzept der Namens- und Rechte-Hierarchie

Die wichtigste Sicherheitskomponente im Domino-System stellt die ID-Datei dar. In dieser Datei sind die wichtigsten Informationen zu dem Benutzer und seiner Stellung im Domino-Rechte-System gespeichert.

Die Rechte-Hierarchie hat an ihrer Spitze die Zulassungsstelle des Unternehmens (die Organisation – abgekürzt: O). Deshalb trägt sie in der Regel auch den Namen des Unternehmens. Darunter können verschiedene Ebenen an Unterorganisationen und darunter die Benutzer und Server angesiedelt sein. Die Unterorganisationen bezeichnet Domino als „Organisation Units (OU). Die Zulassung einer Unternehmenseinheit, einer Person oder eines Servers erfolgt jeweils durch die nächst höhere Ebene. Die Unterorganisationen sind selbst wieder Zulassungsstellen. Bis zu vier Ebenen an Unterorganisationen sind möglich. Die Namen der Benutzer enthalten alle Unternehmensstufen. Dadurch kann eine sehr genaue Namensgebung erfolgen, auch wenn es mehrere Personen mit gleichem Namen in einem Unternehmen gibt.



Zulassungsstellen

Der Name einer Person kann also beispielsweise heißen: Peter Müller/Werkstatt/Halle7/Werk Um/Fertigung AG. Dieser Name ist sicher sehr genau, hat aber auch den Nachteil, dass er sehr lang und unhandlich ist. Deshalb sollten nur so viele Stufen an Unterorganisationen gebildet werden, wie zur Bildung einheitlicher Namen erforderlich sind.

❶❷❸ Ausführungsschritte:

Eine Abteilungs-Zulassungsstelle wird wie folgt erstellt:

1. Administrator-Client starten
2. Das Register „Konfiguration“ und das Werkzeug „Registrierung - Unterorganisation“ anklicken.
3. Zulassungsstelle bestätigen
4. Name und Kennwort der Abteilungs-Zulassungsstelle, Sicherheitstyp und Administrator angeben.
5. Registrieren
6. Mit Hilfe der neuen Zulassungs-ID können jetzt Server und Personen registriert werden.

❶❷❸

Die Namens-Hierarchie unter Lotus Domino richtet sich nach der X.500-Spezifikation und hat folgende Elemente:

- **CN (Common Name = gewöhnlicher Name)**
  Der komplette Vor- und Zuname einer Person bzw. eines Servers.
- **OU1 – 4 (Organisation Unit)**
  Name der Abteilung oder des Unternehmensbereiches. Es sind 4 Abstufungen möglich.
- **O (Organisation)**
  Name des Unternehmens.
- **C (Country)**
  Name des Landes. Der Name des Landes wird häufig nicht verwendet, um die internationale Verwendung der Domäne nicht einzuschränken.

Ein Name muss mindestens einen Namen (CN) und eine Organisation (O) enthalten. Ein Name kann z. B. folgendermaßen aussehen: Peter Meister/Marketing/Deutschland/Grün-AG. In der Langform lautet der Name:

CN=PeterMeister/OU2=Marketing/OU1=Deutschland/O=Grün-AG

In großen Unternehmensinstallationen werden die Server häufig einer eigenen Organisationseinheit zugeteilt (z. B. S1/Server/Unternehmen).

Die Namensbestandteile werden aus den Zulassungsstellen übernommen. Die oberste Zulassungsstelle ist die Organisation (CERT.ID).

Von der Organisation können für die Unterorganisationen auf den verschiedenen Ebenen Zulassungsstellen abgeleitet werden. Die unteren Zulassungsstellen übernehmen automatisch die Namensbestandteile der darüber angeordneten Zulassungsstellen.

Um auf alle Namen einer Zulassungsstelle zu verweisen, wird an die Stelle des Namensbestandteils der Zulassungsstelle ein Stern (*) eingesetzt. Die Namen innerhalb der deutschen Marketingabteilung der Grün AG werden z. B. mit */Marketing/Deutschland/Grün-AG angesprochen. In der Praxis hat sich diese Namensverwendung wenig durchgesetzt. Stattdessen arbeitet man mit Gruppen.

Je nach Zulassungsstelle einer ID-Datei sind die Rechte des Benutzers bzw. Servers auf den Rechte-Bereich dieser Zulassungsstelle beschränkt. Ein Benutzer der Zulassungsstelle Produktion darf nicht ohne weiteres auf einen Server im Bereich der Zulassungsstelle Marketing zugreifen. Dieses Prinzip erlaubt es, die Benutzerverwaltung ganzer Bereiche durch einen Administrator vornehmen zu lassen, der nur Rechte innerhalb der Zulassungsstelle erhält.

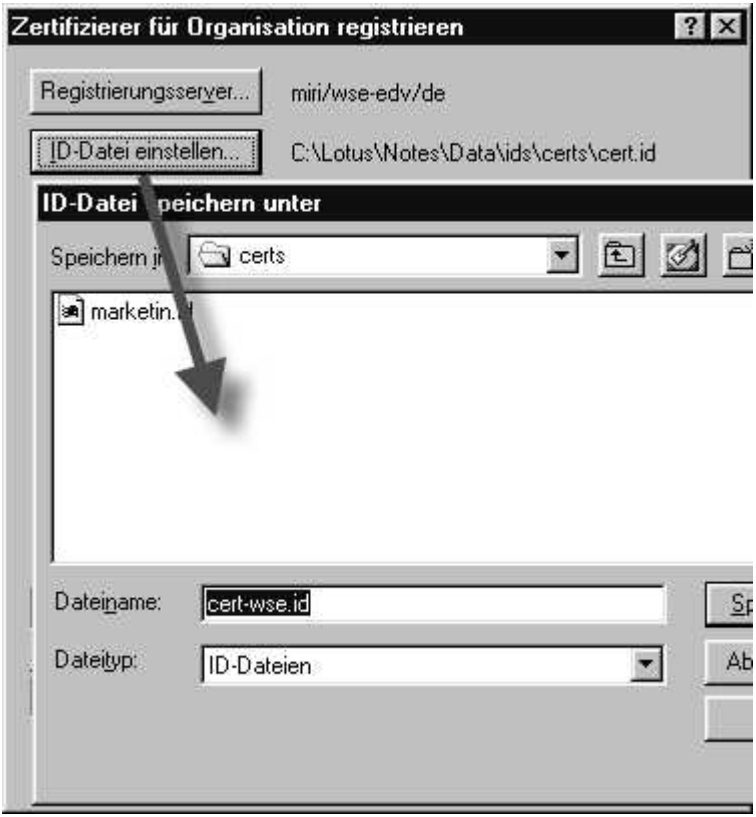
9.2.1 Die Unternehmens-Zulassungsstelle

Wird der erste Server einer Domäne erstellt, so kann in diesem Zusammenhang auch eine ID-Datei für die Zulassungsstelle des Unternehmens erstellt werden. Diese ID-Datei trägt den Namen „CERT.ID“. Der Name kann nachträglich geändert werden (z. B. auf den Namen des Unternehmens).

Es ist aber auch möglich und eventuell erforderlich, eine Unternehmens-Zulassungsstelle über den Administrator-Client anzulegen. Dazu wird der Administrator-Client gestartet und im Register „Konfiguration“ das Werkzeug „Registrieren“ ausgewählt. Darunter findet sich die Position „Organisation“.

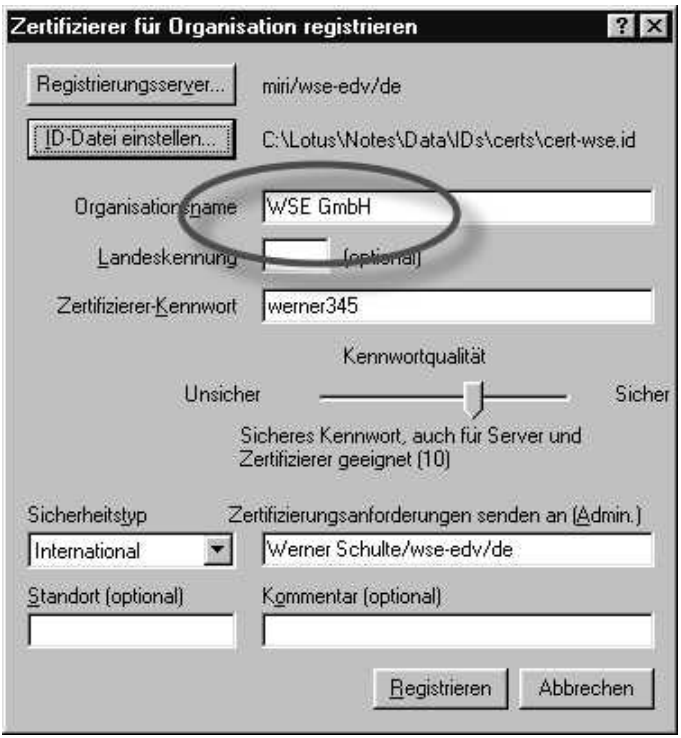
Organisation Registrieren

Wird sie angeklickt, öffnet sich ein Dialog zur Erstellung der Unternehmens-Zulassungsstelle. In diesem Dialogfenster werden die Angaben zur neuen Zulassungsstelle hinterlegt. Zunächst wird der Name der ID-Datei über die Schaltfläche „ID-Datei einstellen“ festgelegt und angegeben, wo sie gespeichert werden soll. Der Vorschlagspfad wird den Administrator-Vorgaben entnommen.



ID-Datei der Zulassungsstelle festlegen

In die nächsten Felder werden der Name der neuen Organisation und das zu verwendende Kennwort eingetragen. Da es sich hier um ein wichtiges Element der Domino-Organisation handelt, sollte die Kennwort-Qualität hoch eingestellt sein. Die Landeskennung wird in der Regel nicht verwendet, um zu vermeiden, dass bei Benutzern aus mehreren Ländern innerhalb einer Organisation bereits ein Land im Unternehmen enthalten ist. Bei der Verschlüsselung entspricht die Einstellung „International“ inzwischen der der „USA“, da der gleiche Verschlüsselungsalgorithmus eingesetzt wird.



Organisation registrieren

Jetzt kann mit Hilfe der Schaltfläche „Registrieren“ die Zulassung durchgeführt werden. Der Administrator-Client erstellt die ID-Datei der Zulassungsstelle und ein Dokument für den Zertifizierer im Domino-Verzeichnis auf dem ausgewählten Registrierungs-Server.

❶❷❸ Ausführungsschritte:

1. Administrator-Client starten
2. Das Register „Konfiguration“ auswählen
3. Unter „Werkzeuge“ die Position „Registrieren“ auswählen
4. Die Position „Organisation“ anklicken
5. Im Dialog „Zertifizierer für Organisation registrieren“ das Windows-Verzeichnis und den Namen für die ID-Datei festlegen
6. Namen der Organisation angeben
7. Kennwort-Qualität und Kennwort festlegen
8. Sicherheitstyp „International“ festlegen
9. Administrator angeben
10. Registrieren

❶❷❸

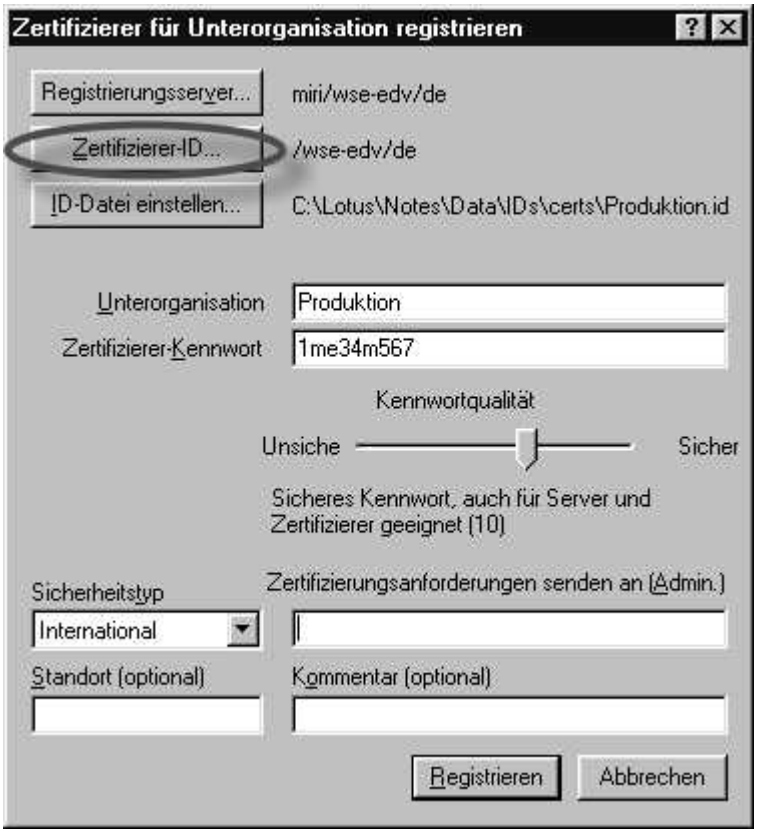
Die neue Zulassungsstelle kann jetzt eingesetzt werden, um Unterorganisationen oder direkt Benutzer und Server zuzulassen.

9.2.2 Unterorganisationen zulassen

Die Zulassung der Unterorganisation findet sich ebenfalls unter „Registrierung“ bei den Werkzeugen im Abschnitt „Konfiguration“ des Administrator-Clients. Die Auswahl der Position „Unterorganisation“ löst eine Abfrage nach dem Kennwort für die Zulassungsstelle aus. Der Name der Zulassungsstelle wird den Administrator-Vorgaben entnommen. Diese Vorgaben können vor der Registrierung geändert werden. Ein Abbruch der Kennwort-Eingabe führt zur Auswahl einer geeigneten Zulassungs-ID-Datei.

Kennwort-Abfrage der Zulassungsstelle

Im folgenden Dialogfenster sind die gleichen Angaben zu machen, wie bei der Organisation. Zusätzlich ist hier die Zulassungsstelle mit aufgeführt.



Unterorganisation registrieren

Über die Schaltfläche „Zertifizierer-ID“ kann die Zulassungsstelle ebenfalls geändert werden. Auch dieser Dialog wird über „Registrieren“ abgeschlossen.

❶❷❸ Ausführungsschritte:

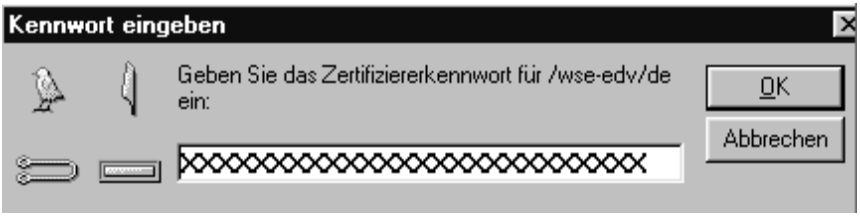
1. Administrator-Client starten
2. Unter „Konfiguration / Werkzeuge“ die Position „Registrieren“ aufklappen
3. „Unterorganisation...“ auswählen
4. Kennwort für die Zulassungsstelle eingeben oder Zulassungsstelle wechseln
5. Im Dialog „Zertifizierer für Unterorganisation registrieren“ den Registrierungs-Server oder die Zulassungsstelle ändern, falls erforderlich
6. Den Namen und das Verzeichnis für die ID-Datei der Unterorganisation bestimmen
7. Name, Kennwort-Qualität und Kennwort für die Unterorganisation festlegen
8. Sicherheitstyp auf „International“ setzen
9. Registrieren

❶❷❸

Bevor die einzelnen Benutzer registriert werden, sollten zunächst alle erforderlichen Unterorganisationen in den notwendigen Ebenen angelegt sein. Zur einfacheren Verwaltung können auch für Server eigene Unterorganisationen erstellt werden.

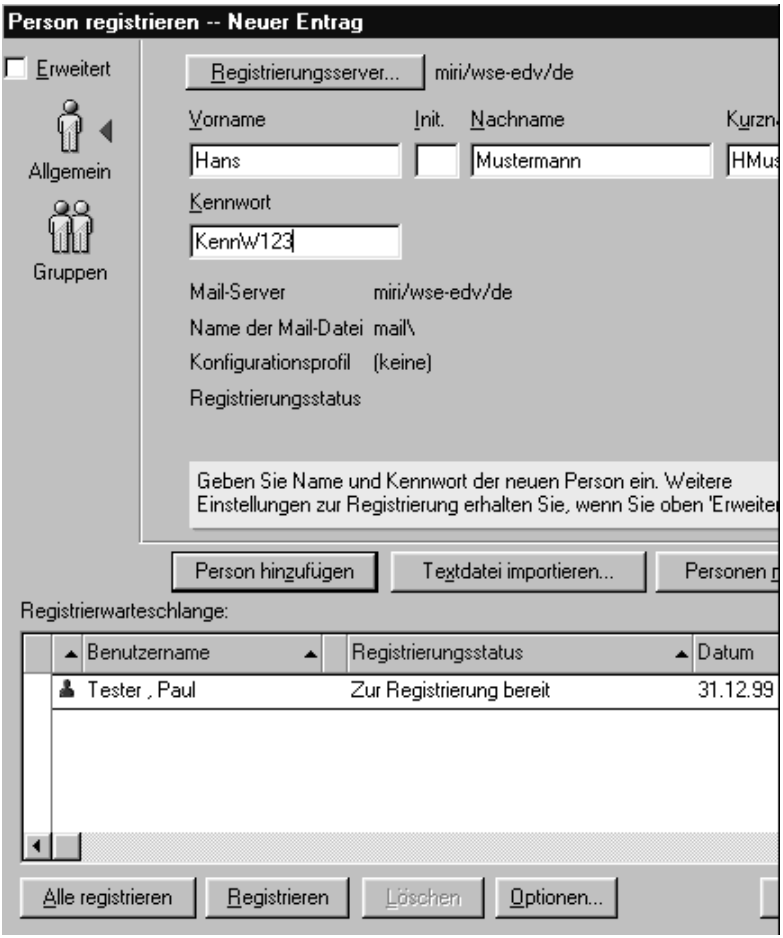
9.3 Benutzerverwaltung

Zur Registrierung eines neuen Benutzers bietet Domino im Administrator-Client unter dem Register „Personen und Gruppen“ das Werkzeug „Personen / Registrieren“. Bevor jedoch die eigentliche Registrierung beginnt, wird das Kennwort des Zertifizierers abgefragt.



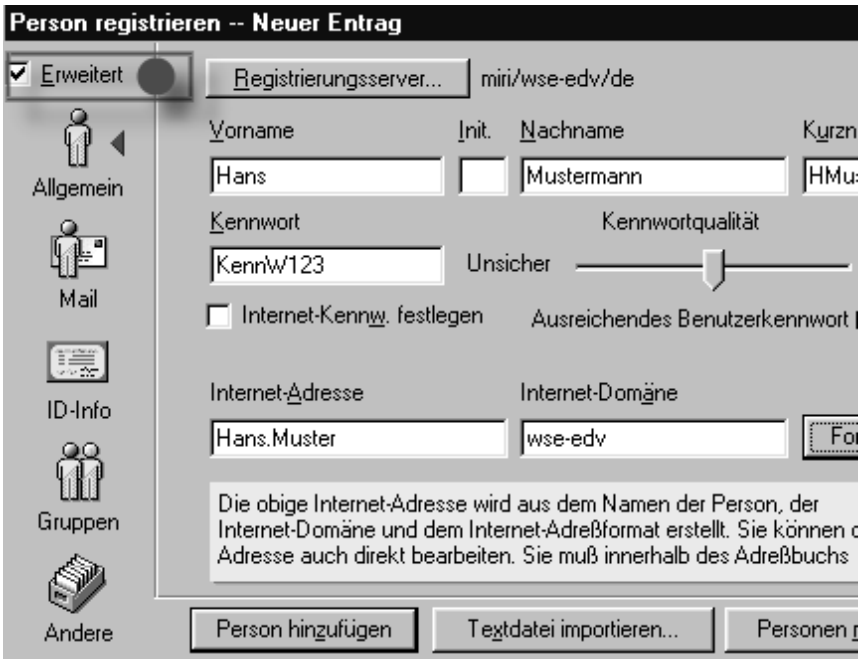
Kennwortabfrage

Die Registrierung kann auf zwei Arten verwendet werden: mit vielen Vorgabewerten und wenigen Angaben oder in der Form „Erweitert“.



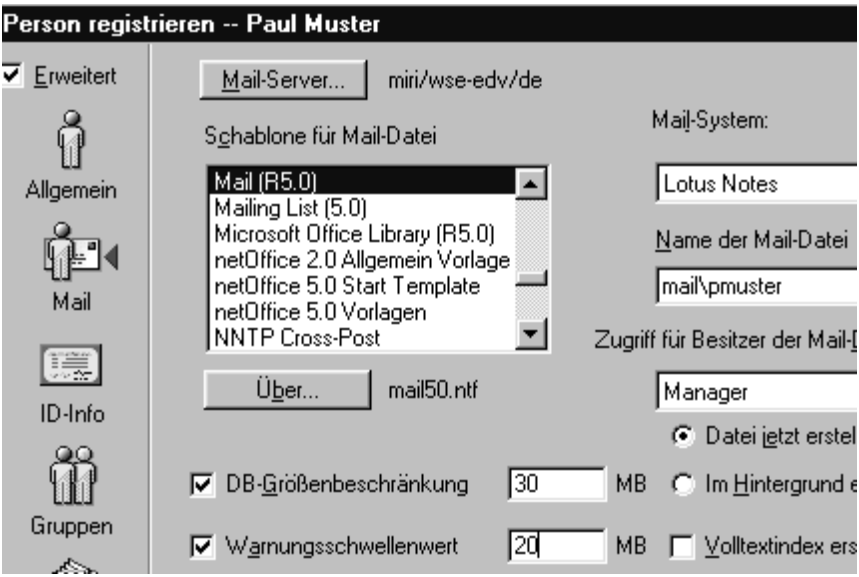
Standardversion der Registrierung

Lediglich Name, Kurzname und Kennwort sind erforderlich, um die Person mit Hilfe der Schaltfläche „Person hinzufügen“ in die Registrierwarteschlange aufzunehmen. Bei der Registrierwarteschlange handelt es sich um eine Datenbank mit dem Namen „userreg.nsf“. In dieser Datenbank werden die Personendaten zwischengespeichert, bis sie mit „Registrieren“ endgültig angelegt werden. Registrieren bedeutet, dass ein Personendokument im Domino-Verzeichnis, eine Benutzer-ID und eine Mail-Datei angelegt werden.



Erweiterte Personenregistrierung

Wird die erweiterte Version der Registrierung gewählt, nimmt die Anzahl der Abschnitte und Felder, die ausgefüllt werden können, erheblich zu. Die Abschnitte „Mail“, „ID-Info“ und „Andere“ erscheinen zusätzlich im Dialogfenster. Im Abschnitt „Allgemein“ sind jetzt die Felder „Kennwortqualität“, Internet-Kennwort und Internet-Adresse verfügbar.



Abschnitt „Mail“ der Benutzerregistrierung

Im Abschnitt „Mail“ werden Angaben zu der Mail-Datenbank des neuen Benutzers definiert.

- Mail-Server

  Standardmäßig wird der Mail-Server aus den Administrationsvorgaben verwendet.

- Datenbankschablone

  Der Name der normalen Mail-Schablone ist „Mailxx.nsf“, wobei xx die Version (z.B. 50 für 5.0) bedeutet.

- Mail-System

  Lotus Notes, Internet (POP oder IMAP) oder anderes Mail-System

- Name der Mail-Datei

  Als Standard wird das Verzeichnis „mail“, der erste Buchstabe des Vornamens und 7 Zeichen des Nachnamens verwendet. Der Name der Mail-Datei wird im Personendokument und in der Arbeitsumgebung des Benutzers hinterlegt und kann dort geändert werden.

- Zugriffsrechte des Benutzers auf die Mail-Datei

  Werden die Zugriffsrechte heruntergesetzt, so wird der aktuelle Administrator als Manager zu der Liste der zugriffsberechtigten Personen hinzugefügt.

- Größenbeschränkung der Mail-Datenbank

  Wichtig für Personen, die nie ihre e-Mails löschen!

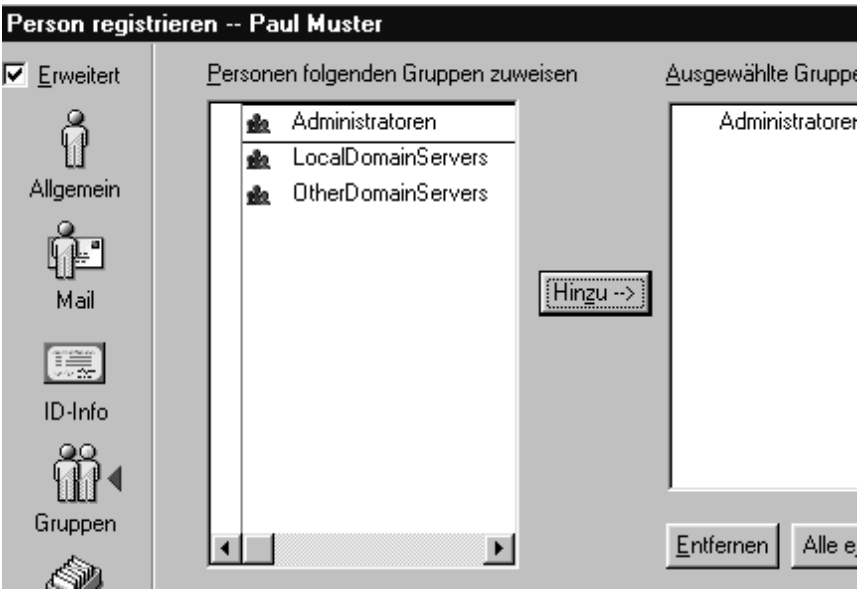
- Warnungsschwellenwert

  Zur Vorwarnung des Benutzers.

- Volltextindex

  Wenn die Mail-Datenbank einen Volltextindex erhalten soll.

Direkt bei der Registrierung kann eine Person bereits bestimmten Gruppen zugeordnet werden. Die Möglichkeit ist sehr schnell und einfach und wird deshalb häufig genutzt.

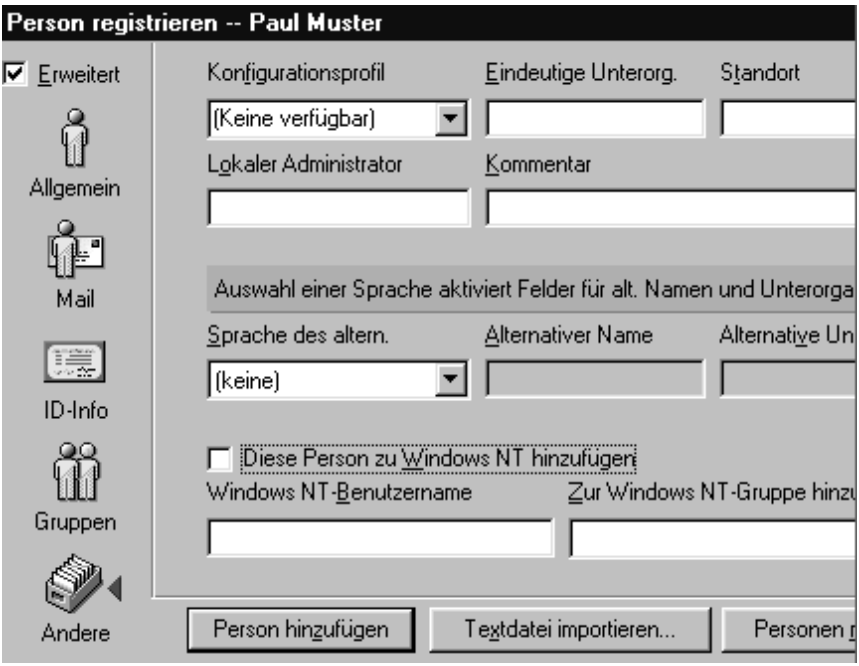


Gruppen zuweisen

Im Abschnitt „ID-Info“ werden das Ablaufdatum für die ID und der Speicherort der ID-Datei eingestellt.

ID-Info des Benutzers

Eine Reihe weiterer Angaben finden sich im Abschnitt „Andere“. Die wichtigsten beziehen sich auf die Verbindung zu WindowsNT bzw. Windows2000. Werden diese Felder genutzt, so wird der Benutzer gleichzeitig als Windows-Benutzer angelegt.



Abschnitt „Andere“

Mit „Person hinzufügen“ wird auch hier die Person in die Registrierwarteschlange übernommen und mit Registrieren tatsächlich angelegt.

9.3.1 Benutzer aus einer Textdatei registrieren

Bei der Installation eines Domino-Systems oder bei der Einführung von Lotus Domino in einem neuen Bereich müssen oft sehr viele neue Benutzer gleichzeitig angelegt werden. In diesem Fall ist es sehr mühsam, für jeden einzelnen Benutzer die Daten der Erfassungsmaske einzutippen. Der Administrator-Client bietet für diesen Fall ausführliche Unterstützung an: die Registrierung aus einer Textdatei. Das Prinzip dafür ist ganz einfach. Alle Benutzer, die neu angelegt werden sollen, werden in Form einer Liste in eine Textdatei eingetragen. Bei der Registrierung wird die Textdatei dann automatisch in die entsprechenden Benutzerdaten umgewandelt. Damit das Verfahren angewendet werden kann, sind die gleichen Voraussetzungen erforderlich, wie bei der normalen Benutzerregistrierung über den Erfassungsdialog.

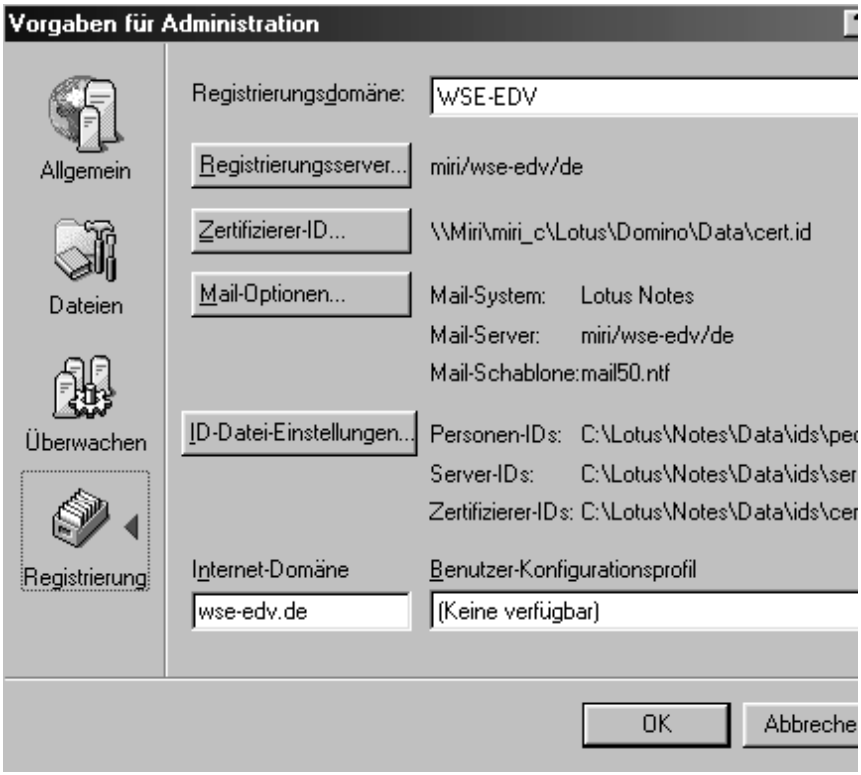
Die Person, die Benutzer anlegt, muss über ausreichende Rechte verfügen. Sie muss das Zertifizierer-Kennwort wissen und Rechte am Domino-Verzeichnis besitzen. Da Mail-Dateien auf dem Server angelegt werden, sind auch hier die entsprechenden Rechte erforderlich.

Zusätzlich können einige Einstellungen vorgenommen werden, wenn die Standardwerte nicht ausreichen:

- Vorgaben für die Administration
- Einträge in der Datei „Notes.ini“
- Spezielle Einstellungen für die zu übernehmende Benutzergruppe

9.3.1.1 Vorgaben für die Administration

Im Menü „Datei“ unter der Position „Vorgaben“ befindet sich die Auswahl „Administration“. Sie öffnet eine Dialogbox zur Einstellung verschiedener Standardwerte, die bei Administrationsvorgängen verwendet werden.



Vorgaben für die Administration

Die Angaben in diesem Dialogfenster können verändert werden und dienen als Vorschlagswerte bei den entsprechenden Vorgängen. Bei der Benutzerregistrierung sind das die Werte:

- Domäne
- Server
- Zertifizierungs-Id
- Mail-System, Mail-Server und Schablone für die Erstellung der Mail-Datenbank der neuen Benutzer
- Verzeichnisse, in die die Id-Dateien der neuen Benutzer gespeichert werden sollen.
- Internet-Domäne
- Konfigurationsprofil

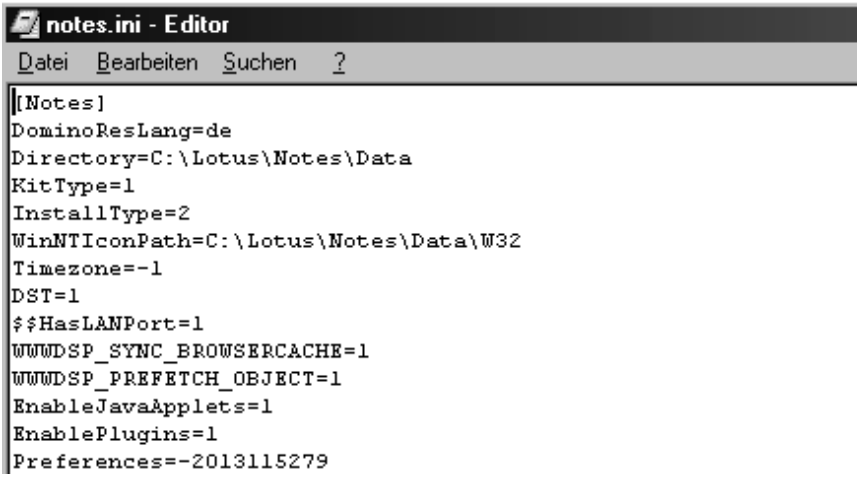
Bei der Registrierung – unter Verwendung des Registrierungsdialoges – werden die Felder aus den Vorgaben für die Administration gefüllt und können überschrieben werden. Wird die Registrierung direkt aus der Textdatei vorgenommen, werden diese Werte automatisch übernommen. Die Inhalte der Textdatei überschreiben, sobald Spaltenwerte eingesetzt sind, alle Vorschlagswerte bei der Registrierung.

9.3.1.2 Steuerdaten in der Datei „Notes.ini“

Eine weitere Quelle für Standardwerte bei der Registrierung von Benutzern stellt die Datei „Notes.ini“ dar. Diese Datei ist eine reine Textdatei und enthält Steuerwerte für viele unterschiedliche Vorgänge im Domino-System. Genau genommen existieren mehrere bzw. viele solcher „Notes.ini“-Dateien. Jeder Server und jeder Client

arbeitet mit einer eigenen „Notes.ini“, die im jeweiligen Notes- bzw. Domino-Verzeichnis zu finden ist. Für die Benutzerregistrierung aus einer Textdatei können folgende Einträge verwendet werden:

- NewUserRegServer
  Server, auf dem der neue Benutzer registriert werden soll.
- CertifierIdFile
  Name und Verzeichnis der Id-Datei, die zur Zertifizierung neuer Benutzer verwendet wird.
- BatchRegFile
  Name der Textdatei, aus der die neuen Benutzer erstellt werden sollen.
- BatchRegSeparator
  Trennzeichen, dass zur Kennzeichnung des Spaltenendes verwendet wird (der Standardwert ist ein Semikolon).



Notes.ini-Einträge

Einträge in der Datei „Notes.ini“ werden beim Start des Clients eingelesen und bleiben während der Sitzung unverändert. Deshalb muss nach einer Änderung der Ini-Einträge der Client neu gestartet werden.

9.3.1.3 Die Textdatei

Die Textdatei kann mit einem beliebigen Texteditor erstellt werden. Jede Zeile in der Datei entspricht einem anzulegenden Benutzer. Jede Spalte entspricht einem Feld im Registrierdialog. Die Reihenfolge der Spalten muss unbedingt eingehalten werden und sieht folgendermaßen aus:

1. Nachname*
2. Name des neuen Benutzers
3. Vorname
4. Initial
5. Abkürzung des zweiten Vornamens
6. Unterorganisation
7. Nur erforderlich, wenn eine hierarchische Struktur verwendet wird.
8. Kennwort*
9. Das Kennwort wird anhand der Kennwortqualität überprüft. Die angegebenen Kennwörter müssen diesen Kriterien entsprechen. Meist wird ein Standardkennwort verwendet, das der Benutzer später ändert.
10. Verzeichnis der Id-Datei

11. Dateiverzeichnis, in das die Id-Datei des neuen Benutzers gespeichert werden soll.
12. Name der Id-Datei
13. Der Name wird standardmäßig aus dem Namen des Benutzers zusammengesetzt, kann aber auch hier speziell angegeben werden.
14. Mail-Server
15. Verzeichnis der Mail-Datei
16. Name der Mail-Datei
17. Der Name der Mail-Datei wird ebenfalls aus dem Namen des Benutzers ermittelt. Wenn der Name der Mail-Datei überschrieben werden soll, kann hier ein Dateiname eingetragen werden.
18. Standort
19. Ergänzende Angabe, wenn zwei E-Mail-Empfänger den gleichen Namen haben.
20. Kommentar
21. Weiterleitungsadresse
22. Adresse, an die die E-Mails des neuen Benutzers standardmäßig weitergeleitet werden sollen.
23. Profilname
24. Benutzer-Konfigurationsprofile enthalten Angaben zu den Einträgen in der Arbeitsumgebung, wenn die Arbeitsstation des neuen Benutzers eingerichtet wird (z. B. Lesezeichen oder Repliken bestimmter Datenbanken).
25. Lokaler Administrator
26. Internet-Adresse

27. Nur erforderlich, wenn die Arbeitsstation des neuen Benutzers über einen Internet-Zugang verfügt und E-Mails direkt abholt bzw. versendet.
28. Kurzname
29. Alternativer Name
30. Alternative Unterorganisation
31. Name der Mail-Datenbank-Schablone
32. Name der Vorlage, die zur Erstellung der Mail-Datenbank verwendet werden soll.

* Diese Felder sind zwingend erforderlich

Achtung!

Die Reihenfolge der Felder muss unbedingt eingehalten werden. Wird ein Feld nicht benutzt, so wird nur das Trennzeichen eingesetzt. Die Angabe von Trennzeichen kann beendet werden, wenn kein Folgefeld mehr gefüllt werden soll.

Beispiel: Name; Vorname; ; ; Kennwort

(Nach dem Kennwort muss kein Trennzeichen mehr angegeben werden, weil kein weiteres Feld gefüllt ist.)

Die Einträge in der Textdatei können jetzt folgendes Aussehen haben:

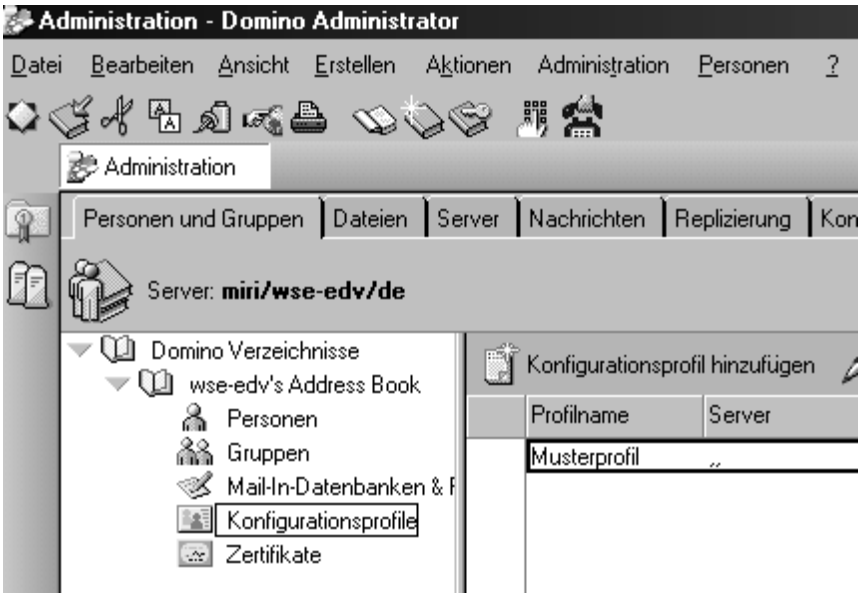
Müller; Klaus; ; ; Kennwort; ; ; ; ; ; ; ; ; Musterprofil

Maier; Anna; ; ; Kennwort; ; ; ; ; ; ; ; ; Musterprofil

Lehmann; Karin; ; ; Kennwort; ; ; ; ; ; ; ; ; Musterprofil

Schulze; Peter; ; ; Kennwort; ; ; ; ; ; ; ; ; Musterprofil

Schuster; Dora; ; ; Kennwort; ; ; ; ; ; ; ; ; Musterprofil



Benutzer-Konfigurationsprofil

Damit die Textdatei im Beispiel verwendet werden kann, muss das Benutzer-Konfigurationsprofil „Musterprofil“ bereits angelegt sein.

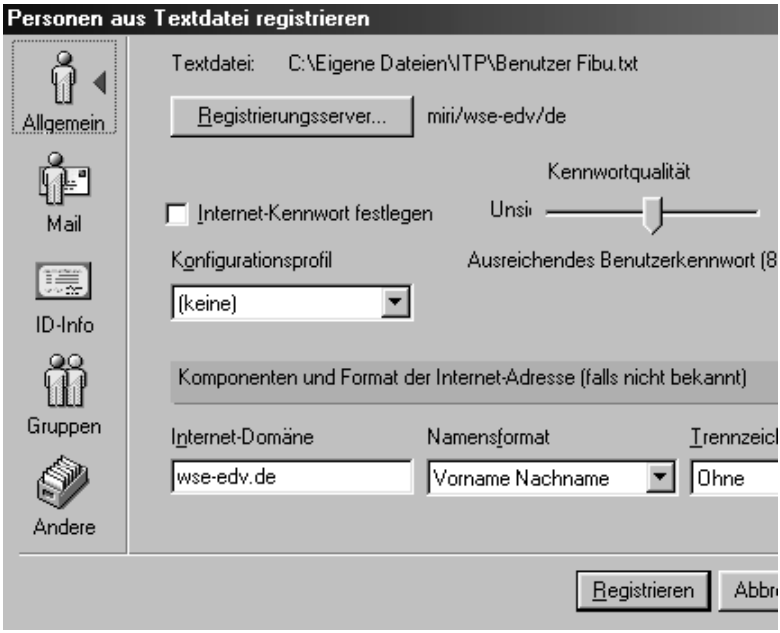
9.3.1.4 Registrieren

Der eigentliche Registrierungsprozess kann auf zwei Arten erfolgen:

- Aus dem Menü „Personen / Personen / Registrieren aus Datei“
- Über die Werkzeugleiste und die Position „Person / Registrieren“

Beide Male wird zunächst das Kennwort der Zertifizierer-Id erfragt.

Soll direkt registriert werden, so erscheint eine Dialogbox mit einigen wenigen Angaben, die mit den Standardwerten vorbelegt sind.

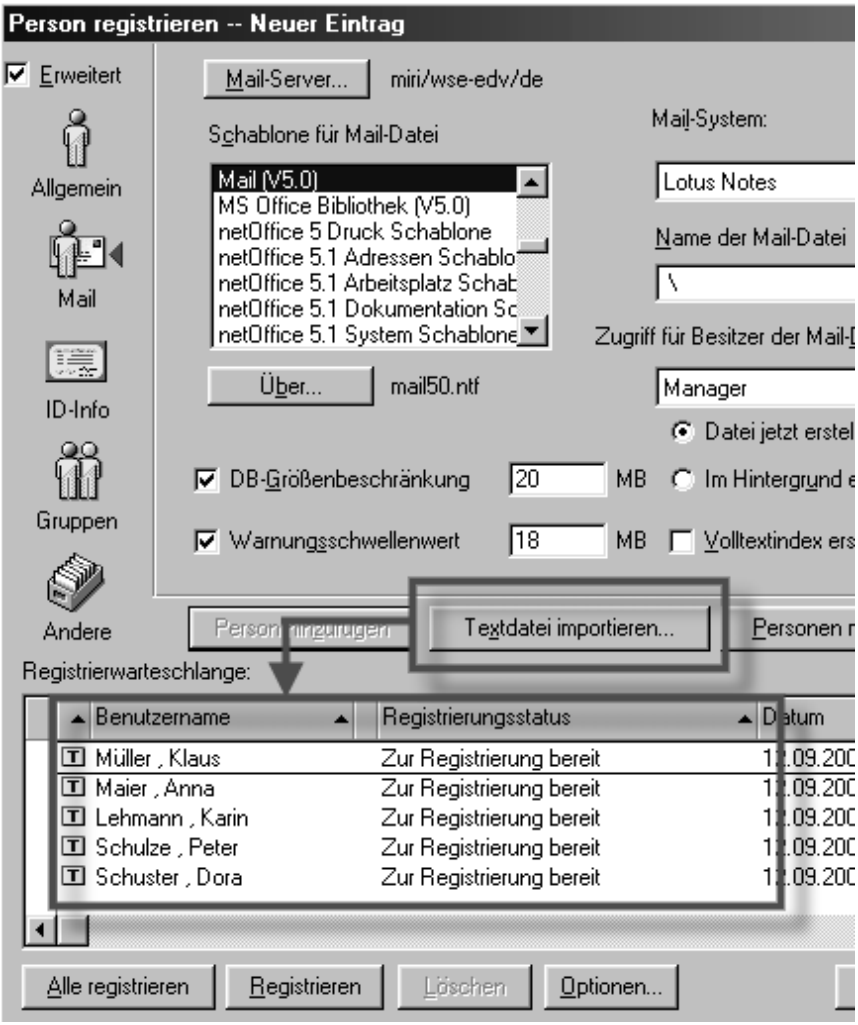


Benutzer aus Textdatei registrieren

Sobald dieser Dialog mit „Registrieren“ verlassen wird, legt der Administrator-Client die neuen Benutzerdokumente im Domino-Verzeichnis an und erstellt die dazugehörigen Id- und Mail-Dateien.

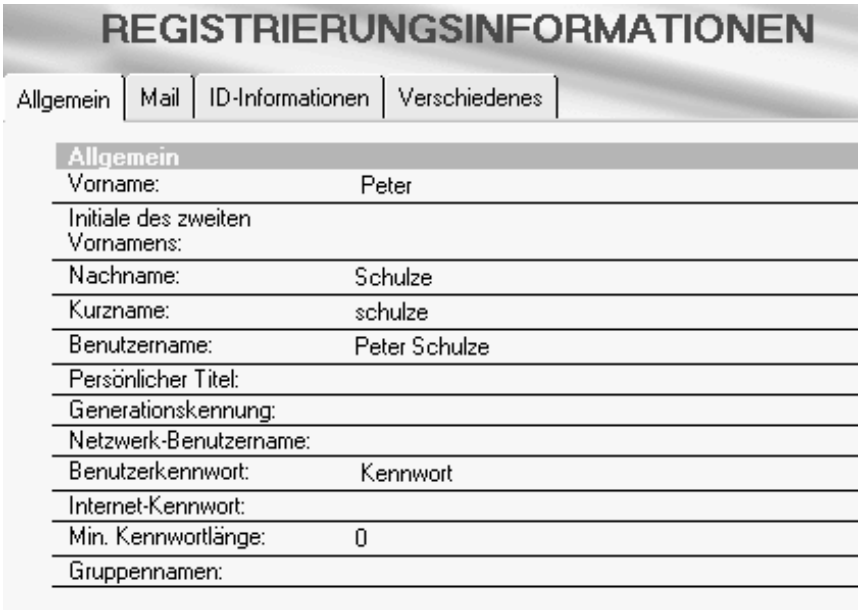
Sollen an den Werten, die über die Textdatei kommen, noch Änderungen vorgenommen und einzelne Benutzerdaten geändert werden, so ist der Weg über die Werkzeugleiste vorzuziehen. Hier erscheint nach der Kennwortabfrage für die Zertifizierungs-Id das gewohnte Dialogfenster für die Registrierung von Personen.

Über die Schaltfläche „Textdatei importieren“ werden die Benutzer in die Registrierwarteschlange übernommen.



Textdatei importieren

Die Registrierwarteschlange ist eine Notes-Datenbank mit dem Namen „UserReg.nsf“ und für jeden Benutzer wird in dieser Datenbank ein Dokument angelegt. Dabei wird überprüft, soweit es möglich ist, ob die Daten der Benutzer in Ordnung sind.



REGISTRIERUNGSINFORMATIONEN

Allgemein | Mail | ID-Informationen | Verschiedenes

Allgemein	
Vorname:	Peter
Initiale des zweiten Vornamens:	
Nachname:	Schulze
Kurzname:	schulze
Benutzername:	Peter Schulze
Persönlicher Titel:	
Generationskennung:	
Netzwerk-Benutzername:	
Benutzerkennwort:	Kennwort
Internet-Kennwort:	
Min. Kennwortlänge:	0
Gruppennamen:	

Dokument der Datenbank „UserReg.nsf“

Sollen jetzt Daten eines Benutzers angepasst werden, so kann er angeklickt und bearbeitet werden. Über die Schaltfläche „Registrieren“ werden, wie gewohnt, die Benutzer angelegt.

Und hier noch einmal der ganze Ablauf zur Registrierung von Benutzern aus einer Textdatei:

❶❷❸ Ausführungsschritte:

1. Voraussetzungen klären
2. Rechte, Vorgaben für Administration, Notes.ini
3. Textdatei mit den Namen der Benutzer und allen Werten erstellen
4. Im Administrator-Client das Personenregister wählen
5. Das Menü „Personen / Personen / Registrieren aus Datei“ auswählen
6. Kennwort für Zertifizierer-Id eingeben
7. den Dialog „Personen aus Textdatei registrieren“ bearbeiten
8. Über die Schaltfläche „Registrieren“ die Benutzer anlegen

oder

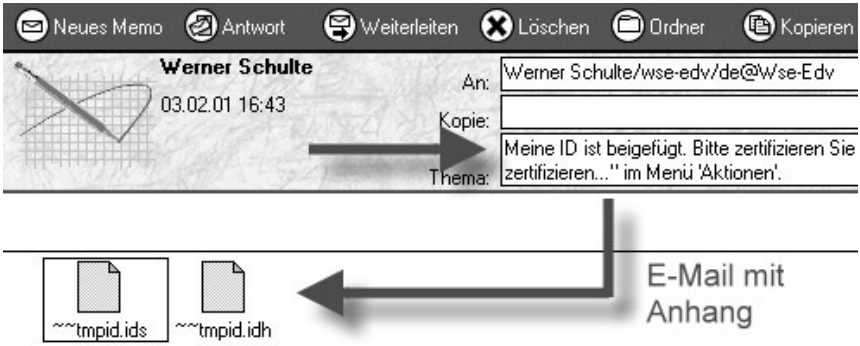
1. Voraussetzungen klären
2. Textdatei erstellen
3. Im Administrator-Client das Personenregister wählen
4. Im Werkzeugfenster die Position „Personen / Registrieren“ wählen
5. Kennwort für Zertifizierer-Id eingeben
6. Den Dialog für die Benutzerregistrierung bearbeiten

7. Mit Hilfe der Schaltfläche „Textdatei importieren“ die Benutzer in die Registrierwarteschlange übernehmen
8. Falls erforderlich – einzelne Benutzerdaten ändern
9. Über die Schaltfläche „Registrieren“ die Benutzer anlegen

Diese Seite ist zur Zeit nicht belegt.

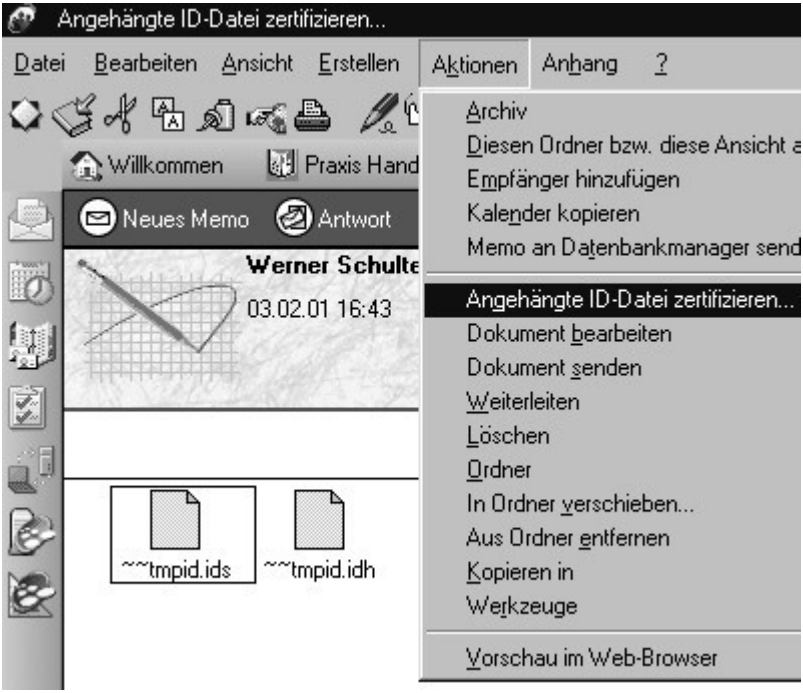
9.3.2 Benutzer-ID erneut zertifizieren

Bei der Registrierung eines neuen Benutzers wird angegeben, wann die ID-Datei ihre Gültigkeit verlieren soll. Deshalb wird eine erneute Zertifizierung der Benutzer-ID angefordert, wenn dieser Fall eintritt. Der erste Schritt zur neuen Zertifizierung geht in diesem Fall vom Benutzer aus. Er erhält von Domino die Meldung, dass seine Benutzerdatei zum Ablaufdatum ungültig wird. Er muss jetzt dafür sorgen, dass ein Administrator seine Benutzer-ID mit einer neuen Geltungsdauer versieht. Dazu wird im Menü „Datei / Extras / Benutzer-ID“ die Schaltfläche „Zertifikat anfordern ...“ angeklickt und die jetzt erscheinende Zertifikatsanforderung an den Administrator geschickt.



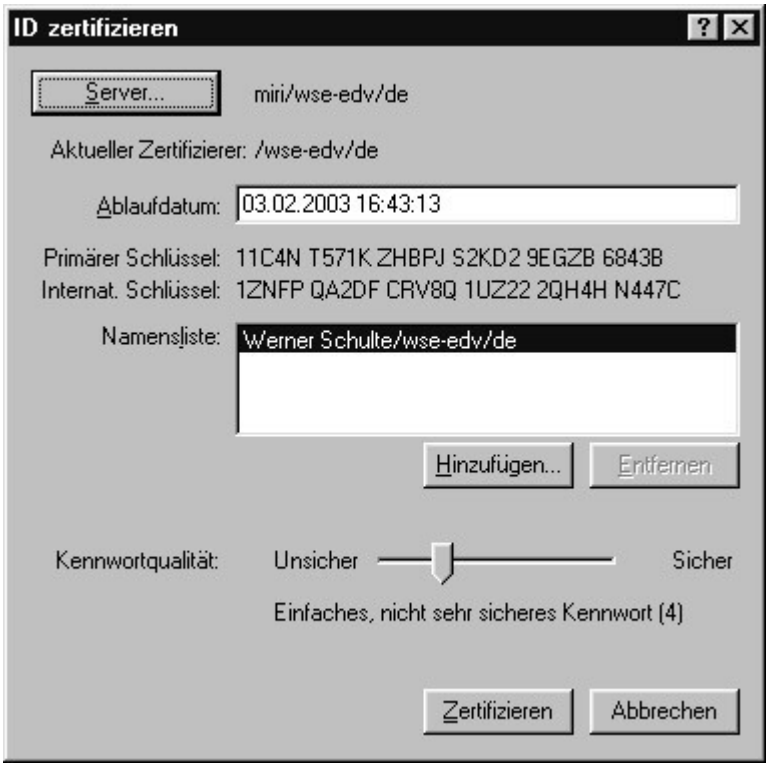
e-Mail mit anhängender ID-Datei

Der Administrator löst die angehängte ID-Datei über das Menü „Aktionen / Angehängte ID-Datei zertifizieren ...“ ab.



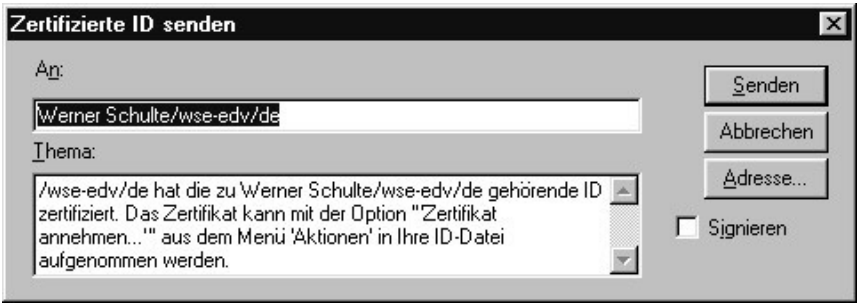
Angehängte Datei zertifizieren ...

Im darauf folgenden Dialog erneuert er die Benutzerregistrierung mit einem neuen Datum.



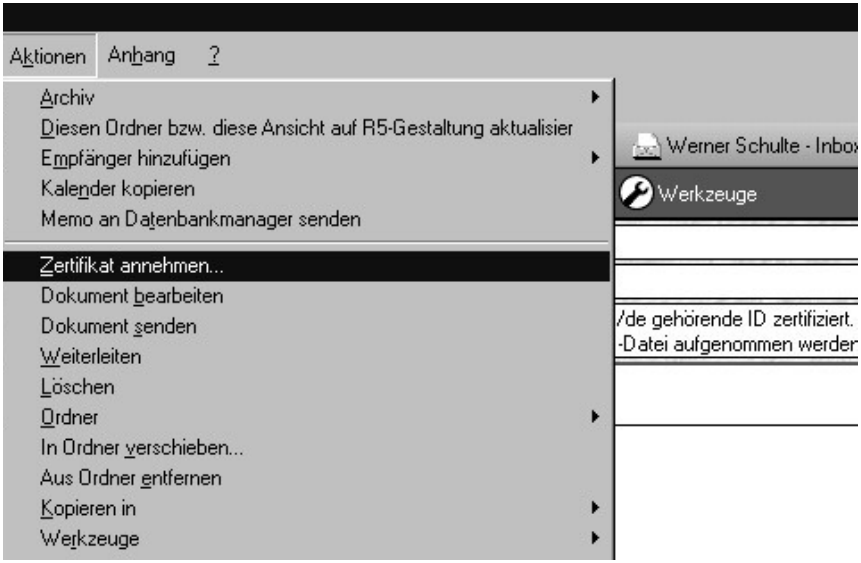
ID-Datei mit neuem Datum zertifizieren

Als Anhang an die automatisch erzeugte e-Mail sendet er die ID-Datei an den Benutzer zurück.



Automatische Antwort als e-Mail mit Anhang

Der Benutzer wird aufgefordert, die Datei mit der Menüposition „Aktionen / Zertifikat annehmen“ zu speichern.



Zertifikat annehmen

Damit ist die erneute Zertifizierung abgeschlossen. Die ID-Datei kann bis zu ihrem neuen Ablaufdatum verwendet werden.

❶❷❸ Ausführungsschritte:

1. Benutzer sendet die ID-Datei per e-Mail.
2. Mit Hilfe der Schaltfläche „Angehängte Datei zertifizieren ...“ den Zertifizierungsvorgang starten.

3. Im Dialog „ID zertifizieren“ das neue Datum eintragen und die Schaltfläche „Zertifizieren“ anklicken.
4. Die ID-Datei an den Benutzer zurücksenden.

9.4 Das Personen- und das Gruppendokument im Domino-Verzeichnis

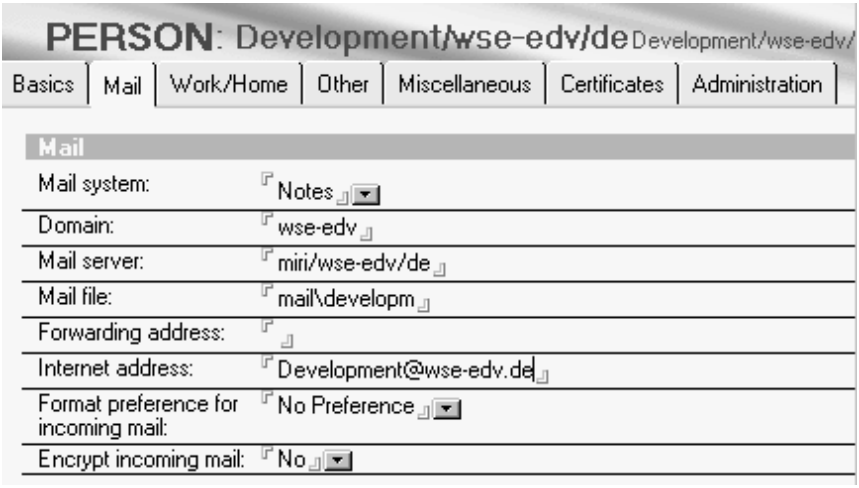
Mit der Registrierung wird ein Dokument im Domino-Verzeichnis der Domäne (names.nsf) angelegt. Das Personendokument hat die Aufgaben:

- Adressierung, Versand- und Eingangssteuerung von e-Mails
- Adressverzeichnis der Benutzer
- Unterstützung der Benutzerverwaltung

Im allgemeinen Abschnitt werden Namen, Adressen und das Internet-Kennwort hinterlegt.

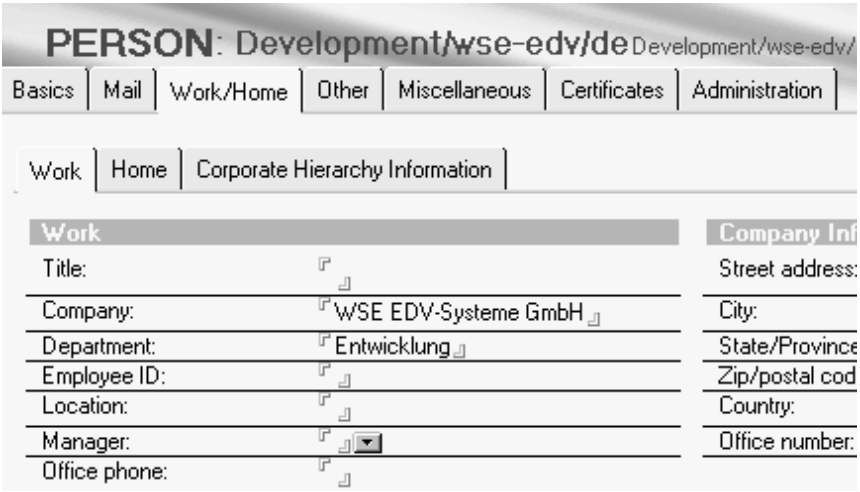
Register „Allgemein“ des Personendokumentes

Das „Mail“-Register beinhaltet Angaben zu der Domäne, dem Mail-System, dem Mail-Server und der Mail-Datei des Benutzers.



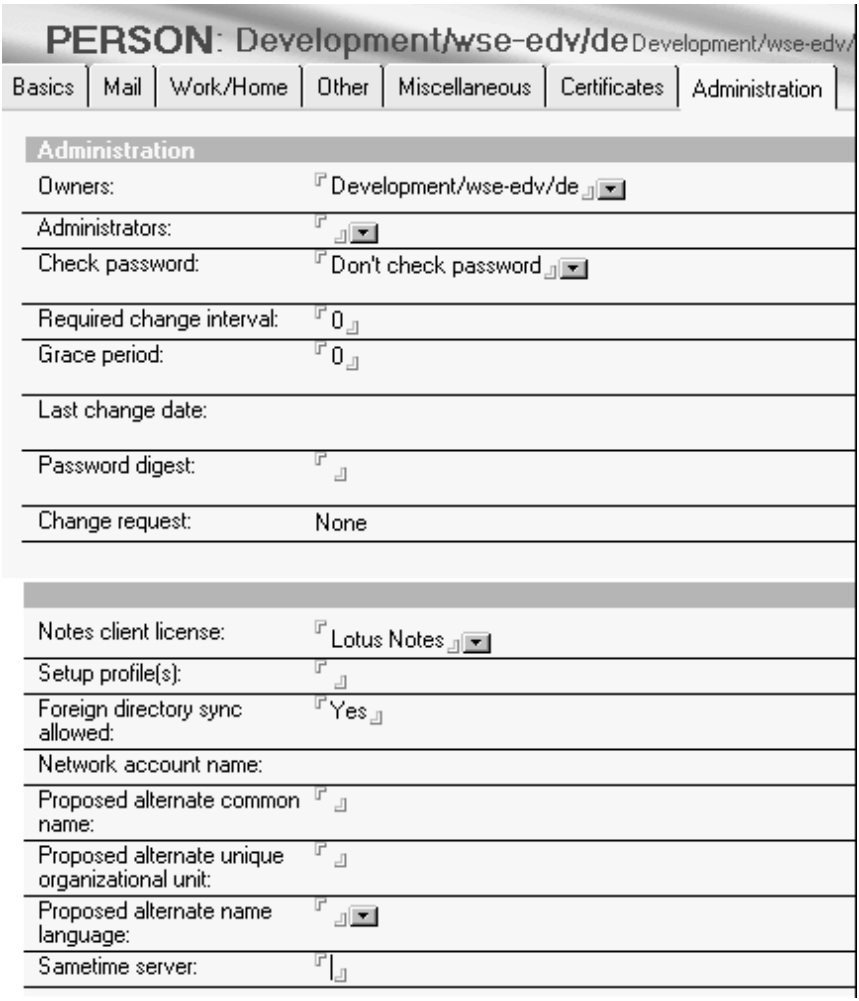
Register „Mail“ des Personendokumentes

Je eine Adresse für die Firma und für die private Anschrift können bei der Person gespeichert werden.



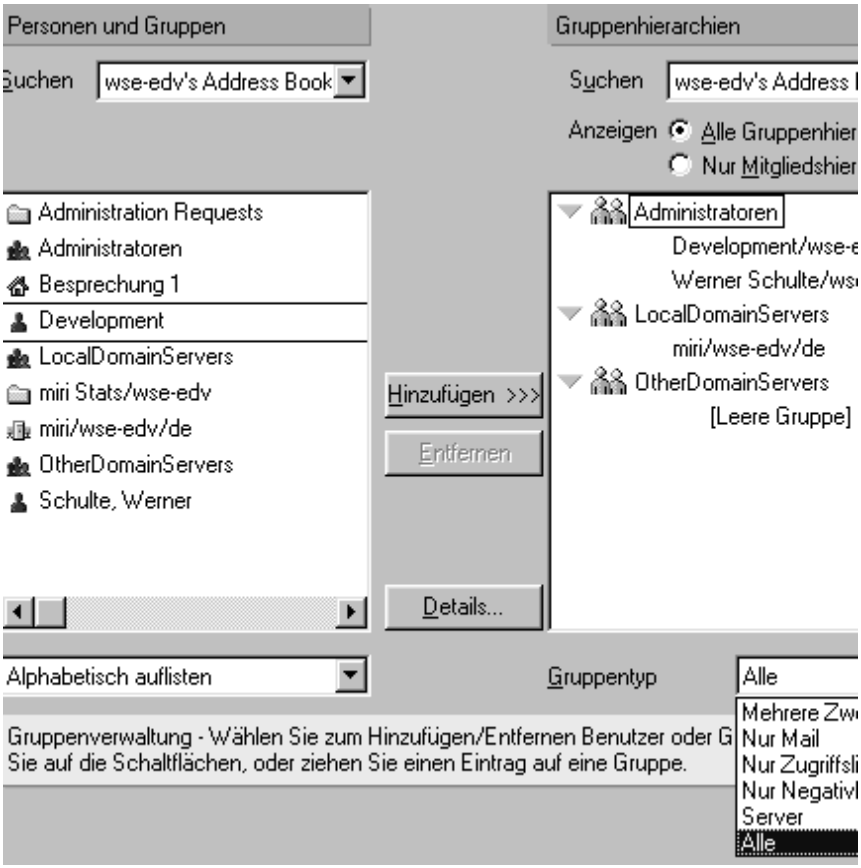
Adressen-Register des Personendokumentes

Bei der Administration des Personendokumentes ist die Definition einer Kennwortprüfung möglich. Dabei wird angegeben, wie lange das Kennwort Gültigkeit haben und die Vorwarnzeit sein soll.



Register „Administration“ des Personendokumentes

Im Feld „Notes Lizenz“ wird angegeben, welche Art von Lizenz (Notes, Mail, Desktop, Designer, Administration) der Benutzer hat. Da die tatsächlichen Funktionen, die ein Benutzer verwenden kann, von den installierten Client-Programmen abhängen, hat dieses Feld nur noch statistische Bedeutung.



Gruppen verwalten

Zur bequemen Verwaltung von Gruppen findet sich in der Werkzeugleiste des Administrator-Clients ein Dialog, in dem links die vorhandenen Gruppen und Personen und rechts die möglichen Gruppen aufgeführt sind. Nach dem Auswählen der Person und der gewünschten Gruppe wird über die „Hinzufügen >>>“-Taste die Person einer Gruppe hinzugefügt. Die Schaltfläche „Details“ zeigt das Dokument der gerade ausgewählten Person oder Gruppe.

Das Gruppendokument

Eine neue Gruppe wird ebenfalls über die Werkzeugleiste angelegt. Neben Name und Beschreibung wird ein Gruppentyp angegeben:

- Verschiedene Zwecke
- Nur für Zugriffskontroll-Listen
- Nur e-Mail
- Nur Server
- Nur Negativliste

9.5 Domino als Zertifizierer für das Internet

Es kommt immer häufiger vor, dass nicht nur Notes-Clients der eigenen Domäne, sondern auch fremde Benutzer auf Daten eines Domino-Servers zugreifen sollen. So könnte es z.B. sein, dass ein Kunde Artikel-Dokumentationen lesen oder ein Lieferant aktuelle Preise und Lieferzeiten eintragen soll. In jedem Fall wäre es dann schön, wenn die Informationen direkt in Domino-Datenbanken gespeichert wären und die eigenen Benutzer für den Umgang mit diesen Daten ihre gewohnte Umgebung nicht verlassen müssten. In einer solchen Situation spielt die Sicherheit beim Datenzugriff eine große Rolle. Auch wenn Mitarbeiter einer Außenstelle das Internet als Zugriffsmedium verwenden, darf die Sicherheit nicht außer Acht gelassen werden.

Um die größtmögliche Sicherheit bei solchen Datenzugriffen über das Internet zu gewährleisten, wird das SSL-Protokoll (Secure Socket Layer) verwendet und damit die notwendige Vertrauensbasis in der Kommunikation und Identifizierung für Verbindungen mit einem Domino-Server, der über TCP/IP arbeitet, hergestellt. Ähnlich der ID im Domino-System arbeitet auch SSL mit einem Zertifikat. Dieses Zertifikat wird von einem Zertifizierer der CA (Certificate Authority) ausgestellt. Diese CA garantiert mit ihren Zertifikaten die Vertrauenswürdigkeit der dahinterstehenden Server und Benutzer. Man unterscheidet öffentliche Zertifizierer (z.B. VeriSign) und private Zertifizierer. Das Domino-System kann eine Zertifizierungsstelle für die Verwendung über das SSL-Protokoll zur Verfügung stellen.

Diese Seite ist zur Zeit nicht belegt.

9.5.1 Zertifizierungsstelle anlegen

Zur Erstellung einer Domino-Zertifizierungsstelle für das Internet wird eine Datenbank aus der Schablone „CCA50.NTF" angelegt. Der Name der Datenbank kann beliebig sein und auch für den Titel gibt es keine verbindlichen Vorschriften.

Zertifizierungsdatenbank

Im Startbild der neuen Datenbank sind die Schritte aufgeführt, die jetzt erforderlich sind:

❶❷❸ Ausführungsschritte:

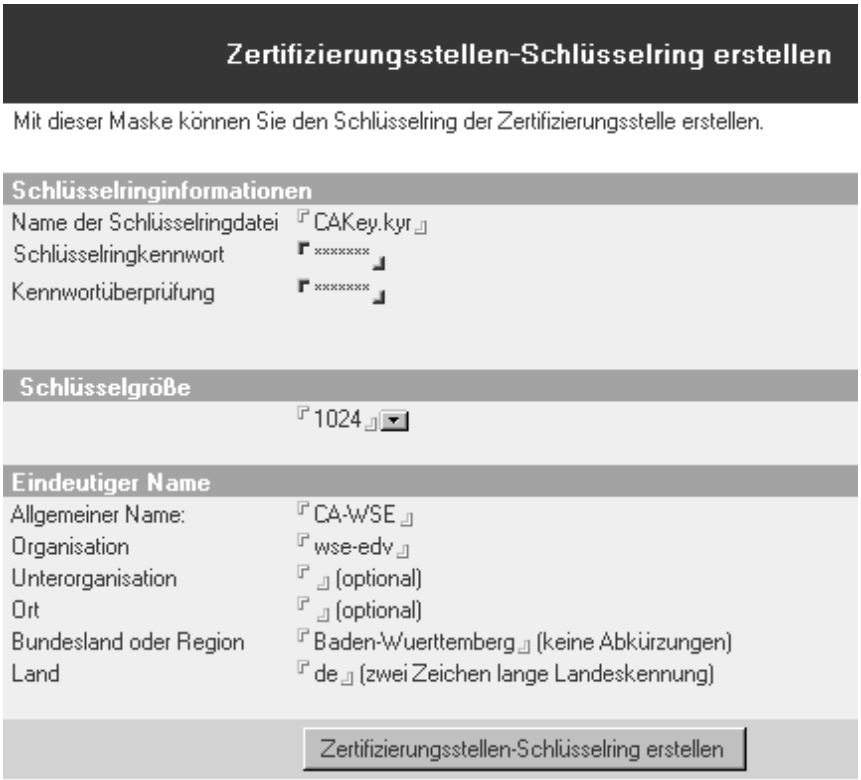
1. Zulassungsschlüsselring & Zulassung erstellen.
2. Zulassungsautoritätsprofil konfigurieren.
3. Server-Schlüsselring & Zulassung erstellen.

❶❷❸

Unter einem Zulassungsschlüsselring ist eine Datei zu verstehen, die in ihrer Funktion der ID-Datei des Domino-Systems entspricht. Sie wird benötigt, um Verschlüsselung und Identifizierung über SSL durchzuführen. In ihr wird das Zertifikat gespeichert. Die Schlüsselringdatei wird standardmäßig in das Datenverzeichnis des Notes-Clients gespeichert. Soll sie an anderer Stelle verwendet werden, muss sie dorthin kopiert oder verschoben werden. Im Übrigen gelten die gleichen Sicherheitsrichtlinien wie bei ID-Dateien unter Lotus Domino.

9.5.1.1 Schlüsselring-Datei und Zertifikat erstellen

Die Schlüsselring-Datei ist der Container für das oberste Zertifikat der neuen Zertifizierungsstelle und enthält deren privaten Schlüssel. Bei der Erstellung werden ähnliche Angaben gemacht, wie bei der Domino-Zulassungsstelle.



Zertifizierungsstellen-Schlüsselring-Datei erstellen

Die Felder der Maske zur Erstellung der Schlüsselring-Datei sind bis auf wenige Ausnahmen zwingend auszufüllen:

- **Name der Schlüsselring-Datei**

  Der Name der Schlüsselring-Datei kann beliebig vergeben werden. Der Vorschlagswert ist „CAKey.kyr".

- **Kennwort, Kennwortprüfung**

  Das Kennwort ist wegen der hohen Sicherheitsrelevanz der Datei mit Vorsicht auszuwählen und an sicherer Stelle zu hinterlegen.

- **Schlüsselgröße**

  Bei der Schlüsselgröße gilt: Je größer der Schlüssel, desto höher ist die Verschlüsselung.

- **Allgemeiner Name**

  Der Allgemeine Name wird in den verschiedenen Programmen angezeigt und sollte die Funktion des Zertifikates erkennen lassen.

- **Organisation**

  Hier kann der Name der Domino-Organisation bzw. der Unternehmensname eingetragen werden.

- **Unterorganisation**

  Optional kann hier ein Teilbereich des Unternehmens angegeben werden.

- **Ort**

  Die Stadt, in der die Organisation der Zulassungsstelle angesiedelt ist.

- **Bundesland oder Region**

  Dieses Feld ist zwingend auszufüllen und soll keine Abkürzung enthalten.

- **Land**

  Landescode (2-stellig) für das Land, in dem die Zulassungsstelle ihren Sitz hat.

Mit Hilfe der Schaltfläche „Zertifizierungsstellen-Schlüsselring erstellen" wird der Vorgang abgeschlossen und die Schlüsselring-Datei erstellt.

❶❷❸ Ausführungsschritte:

1. Über das Menü "Datei / Datenbank / Neu" aus der Schablone "CCA50.NTF" eine Zulassungsdatenbank erstellen. Der Name kann frei gewählt werden.
2. Schlüsselring-Datei für die Zulassungsstelle erzeugen.
3. Die Schlüsselring-Datei sicher speichern, um sie vor Verlust und unberechtigtem Zugriff zu sichern.
4. Ein Zulassungsautoritätsprofil mit den Standardvorgaben für Zertifikate erstellen.

9.5.1.2 Das Zulassungsautoritätsprofil

Bei dem Zulassungsautoritätsprofil handelt es sich um ein Dokument, in dem Standardeinstellungen für die Verwaltung von Zertifikaten hinterlegt werden.

Das Zulassungsautoritätsprofil

Folgende Standardwerte können im Zulassungsautoritätsprofil abgespeichert werden:

- **CA-Schlüsseldatei**

  Der Vorschlagswert für die Speicherung der Schlüsselring-Datei ist das Datenverzeichnis des Administrators, der die Zertifizierungsstelle angelegt hat. Soll diese Datei an einer anderen Stelle gespeichert werden, so muss im Profil die Pfad-Angabe angepasst werden.

- **DNS-Name des Zertifikatsservers**

  Voll qualifizierter Name des Zertifizierungsstellen-Servers, unter dem er über die Namensauflösung eines DNS zu finden ist.

- **SSL für Zertifikatstransaktionen verwenden**

  Der Vorschlagswert für diese Definition ist „Ja", weil Zertifikate sinnvollerweise mit Hilfe von SSL übertragen werden sollten.

- **Anschlussnummer des Zertifikatsservers**

  Der Standardport ist Post 80 und diese Nummer wird verwendet, wenn das Feld leer bleibt. Nur wenn der Server über einen anderen Anschluss arbeitet, muss hier ein Eintrag erfolgen.

- **Bestätigung des signierten Zertifikats an den Antragsteller senden?**

  Wird diese Frage positiv beantwortet, erhält der Anforderer eines Zertifikats eine Bestätigung per e-Mail. Der Vorschlagswert ist „Ja".

- **Sollen signierte Zertifikate in das Domino-Verzeichnis eingetragen werden?**

  Dieser Eintrag in das Domino-Verzeichnis wird standardmäßig vorgenommen. Bei negativer Beantwortung entfällt ein Eintrag.

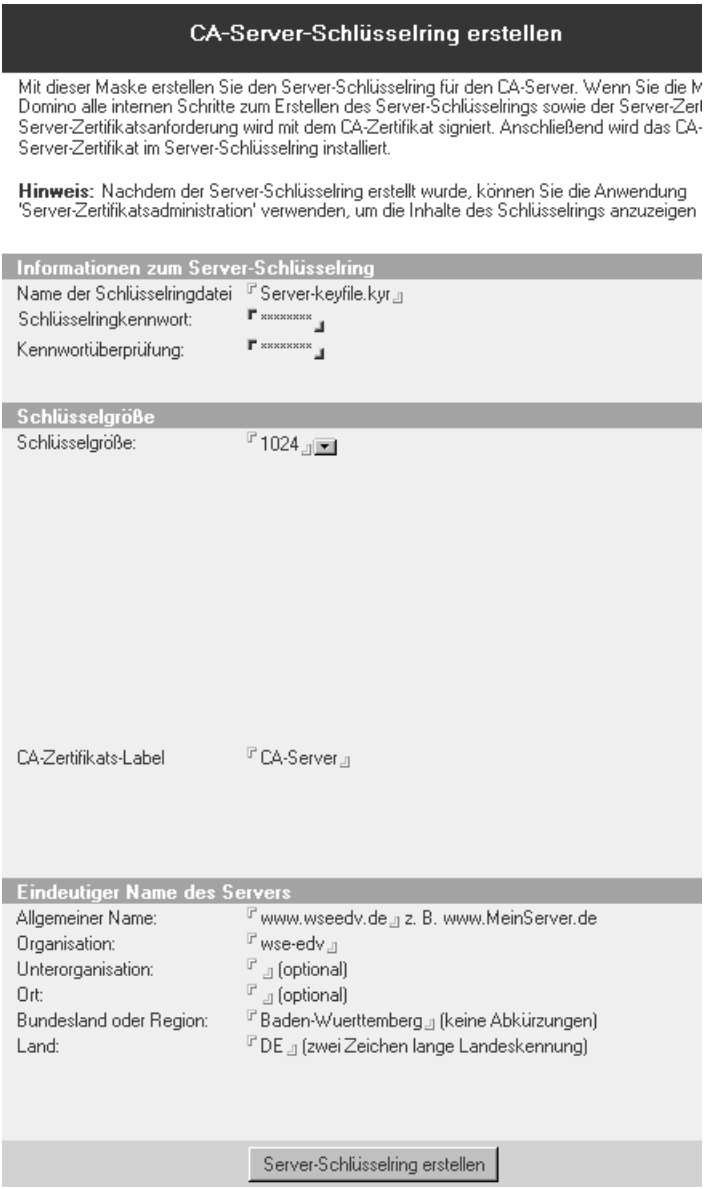
- **Vorgegebener Gültigkeitszeitraum**

  Bei diesem Wert ist zwischen höherer Arbeitsbelastung und höherer Sicherheit zu entscheiden. Der Vorgabewert von zwei Jahren stellt sicher einen vernünftigen Kompromiss dar.

Damit ist das Zulassungsautoritätsprofil definiert und kann mit Hilfe der Schaltfläche „Speichern und schließen" gespeichert werden.

9.5.1.3 Server-Schlüsselring und Zulassung erstellen

Die Zulassungsstelle unterstellt, dass Zertifikatsanforderungen über das SSL-Protokoll und damit von zertifizierten Gegenstellen erfolgen. Deshalb muss auch der Zertifizierungs-Server ein Zertifikat der Zulassungsstelle erhalten.



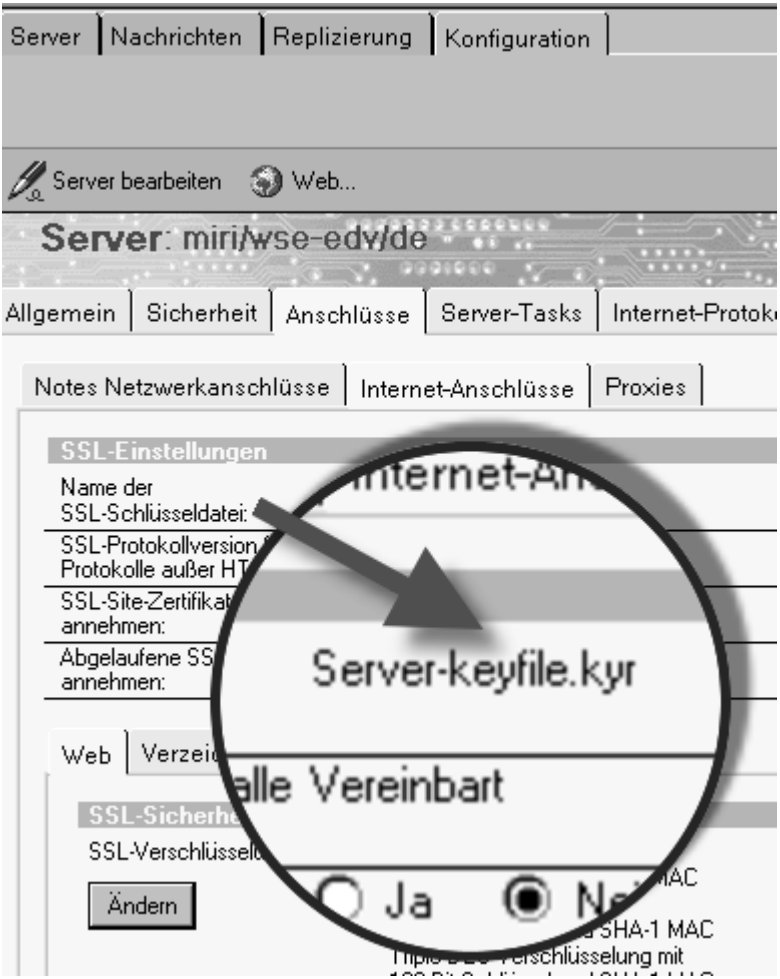
Server-Schlüsselring-Datei erstellen

Der Inhalt entspricht dem der Schlüsselring-Datei der Zulassungsstelle und wird mit Hilfe der Schaltfläche „Server-Schlüsselring erstellen" im Datenverzeichnis des Administrators gespeichert.

Damit der Server über seine Schlüsselring-Dateien verfügen kann, werden sie mit Hilfe des Windows Explorers in das Daten-Verzeichnis des Servers kopiert. Es handelt sich dabei um die Dateien mit gleichem Namen und den Endungen „.kyr" und „sth".

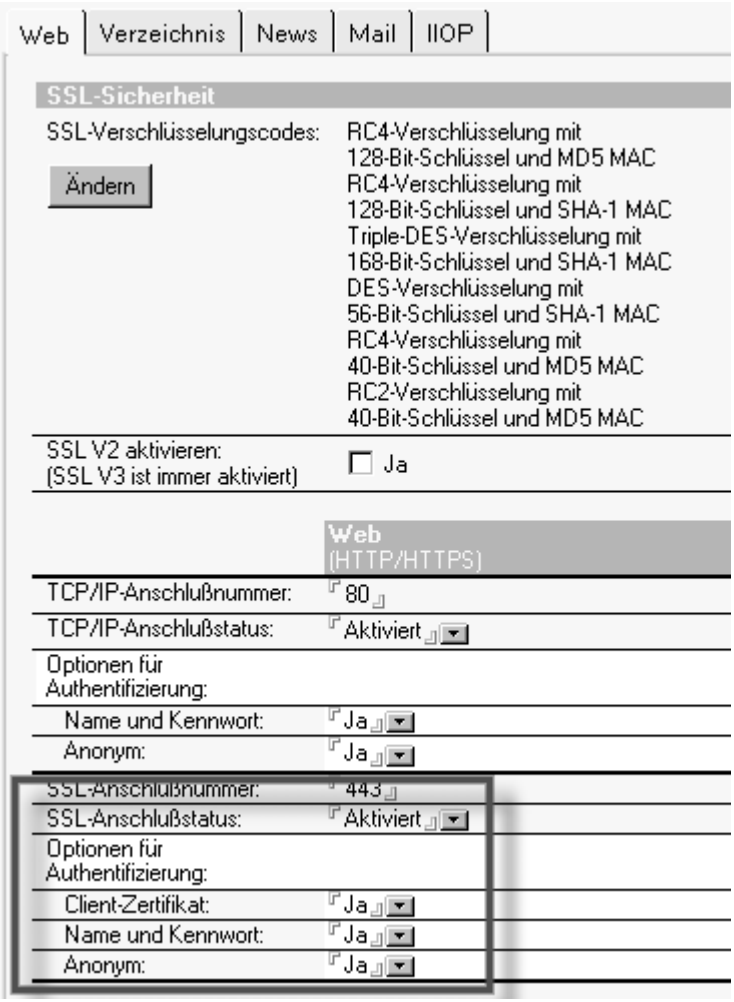
Schlüsselringdateien des Servers

Als Nächstes werden Anpassungen im Server-Dokument vorgenommen. Im Administrator-Client wird unter „Konfiguration" das aktuelle Server-Dokument ausgewählt. Im Register „Anschlüsse" wird im Unterregister „Internet-Anschlüsse" in dem Feld „Name der SSL-Schlüsseldatei" der Name der neu erzeugten Schlüsseldatei des Servers eingetragen.



Schlüsseldatei im Server-Dokument eintragen

Unter dem Register „Web" wird dann der SSL-Anschlussstatus auf „Aktiviert" gesetzt.



SSL-Sicherheitseinstellungen

Bei den Optionen für die Authentifizierung wird neben Kennwort und Name auch das Client-Zertifikat auf „Ja" gesetzt, damit eine zertifizierte SSL-Verbindung für den Datenzugriff vorausgesetzt wird. Damit ist der Schlüsselring-Server betriebsbereit.

❶❷❸ Ausführungsschritte:

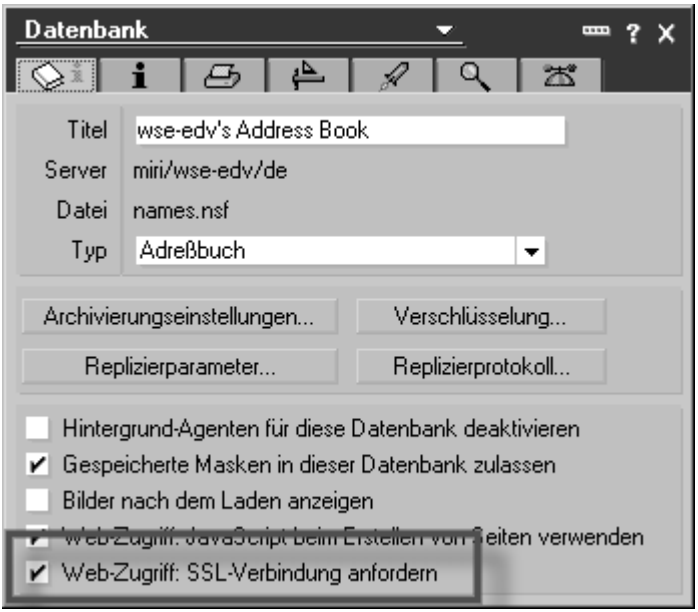
1. Serverschlüsselring-Datei in der Zulassungsdatenbank erzeugen
2. Schlüsselring-Datei des Servers sicher speichern.
3. Kopie der Schlüsselring-Dateien (Endungen ".Kyr" und ".sth" in das Datenverzeichnis des Servers kopieren.
4. Schlüsselring-Datei im Serverdokument des Zulassungsservers eintragen.
5. SSL-Sicherheitsangaben im Server-Dokument des Zulassungsservers bearbeiten.

❶❷❸

Diese Seite ist zur Zeit nicht belegt.

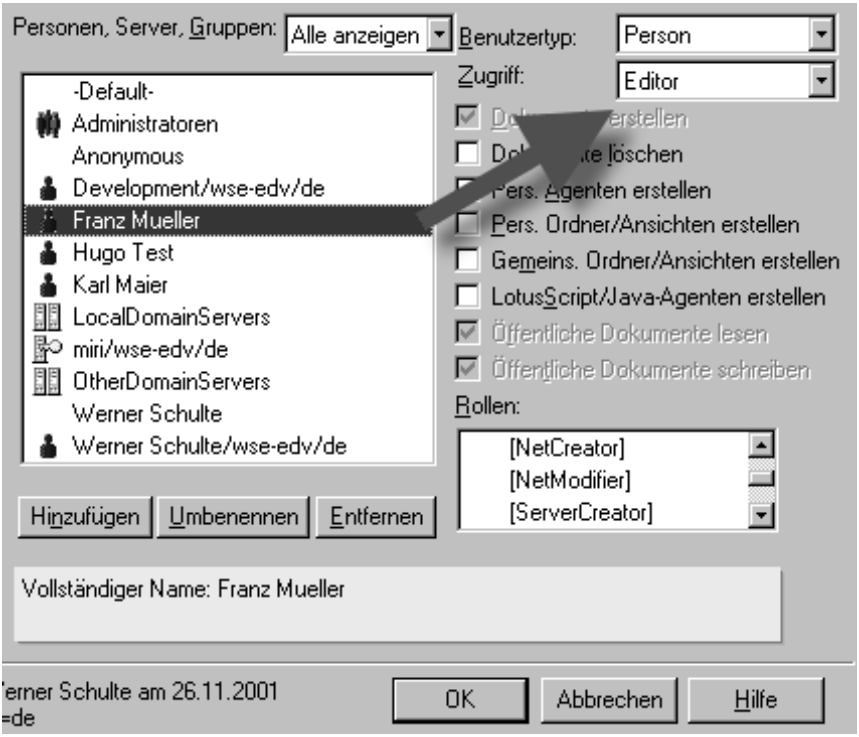
9.5.2 Zertifikate und Zugriffe für Clients

Damit der Zugriff auf eine Datenbank über SSL erfolgen kann, muss das zunächst in den Datenbank-Eigenschaften festgelegt werden.



Datenbank-Einstellungen

Der Benutzer, für den das Zertifikat verwendet werden soll, muss im Domino-Verzeichnis als Benutzer angelegt sein (er muss nicht unbedingt als Domino-Benutzer registriert sein). Danach kann er einzeln oder über eine Gruppe das gewünschte Zugriffsrecht (z.B. Autor) auf die Datenbank erhalten.



Zugriffsrechte

Im nächsten Schritt wird jetzt das Zertifikat für den Benutzer erstellt. Dazu öffnet der Benutzer die Schlüsselring-Datenbank über einen Browser. (Der HTTP-Prozess muss dazu auf dem Server gestartet sein.)

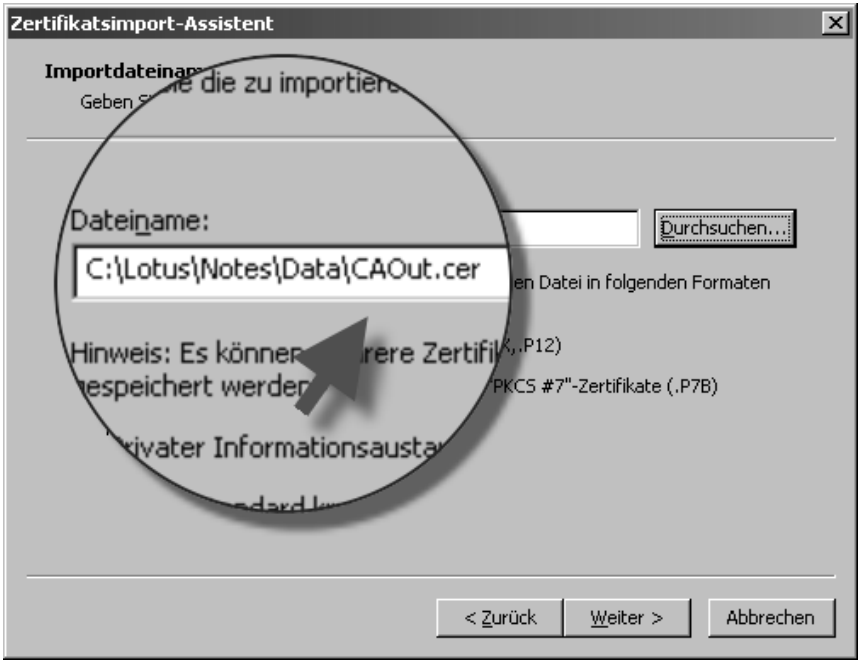
Als ersten Schritt übernimmt er die Zulassungsstelle in seinen Browser. Dazu klickt der Benutzer die Zeile „Diese Zertifizierungsstelle in Ihrem Browser akzeptieren" an.

Zertifizierungsstelle im Browser akzeptieren

Es folgt eine Übersicht über die Daten der Zertifizierungsstelle und eine Zeile zum Akzeptieren. Es erscheint der Download-Dialog für die zu erstellende „.cer”-Datei.

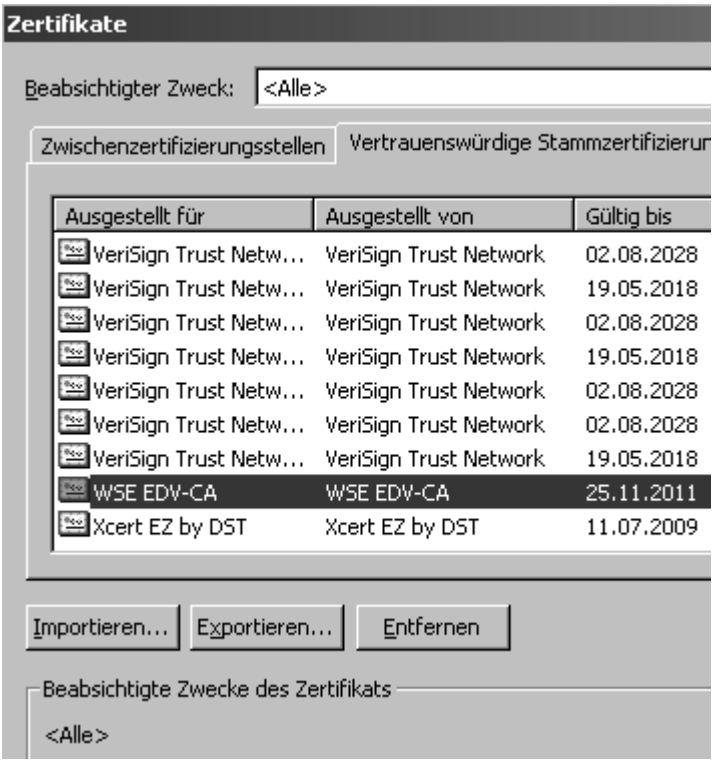
CER-Datei downloaden

Über die Internetoptionen des Browsers wird die CER-Datei importiert und als vertrauenswürdige Zulassungsstelle implementiert.



Zulassungsstelle im Browser importieren

In dem Abschnitt der vertrauenswürdigen Stammzertifizierungsstellen ist jetzt die Zulassungsstelle aus Lotus Domino aufgeführt.



Die neue Stammzertifizierungsstelle im Browser

Für die Benutzer-Zertifikate wird wieder die Zertifizierungsdatenbank über den Browser geöffnet und die Zeile „Client-Zertifikat" angeklickt. Die Maske „Client-Zertifikat anfordern" wird ausgefüllt und abgeschickt.

Client-Zertifikat anfordern

Wird die Schaltfläche „Zertifikatsanforderung einreichen" betätigt, erfolgt eine Bestätigung und der Hinweis auf eine e-Mail-Nachricht, die meldet, dass die Zertifizierung durch den Administrator bestätigt wurde.

Ihre Zertifikatsanforderung wurde eingereicht

Sie erhalten eine E-Mail-Benachrichtigung, wenn die Zertifizierungsstelle Ihre Anforderung geprüft hat.

Dies sind die von Ihnen eingegebenen Kontaktinformationen:

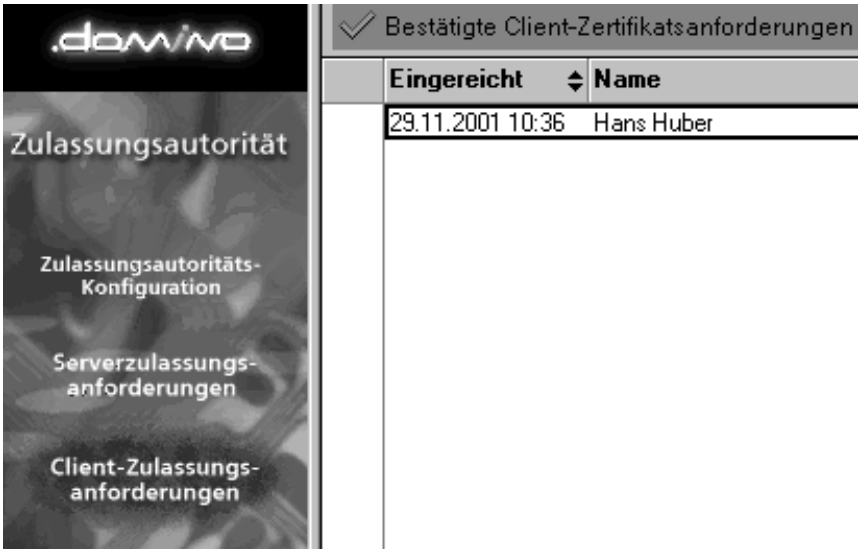
E-Mail-Adresse:	werner.schulte@wse-edv.de
Kommentare:	
Rufnummer:	

Dies sind die Informationen in dem von Ihnen eingereichten Zertifikat:

Allgemeiner Name:	Hans Huber
Organisation:	wse-edv
Unterorganisation:	
Ort:	
Bundesland oder Region:	Baden-Wuerttemberg
Land:	DE
E-Mail	Werner.Schulte@wse-edv.de

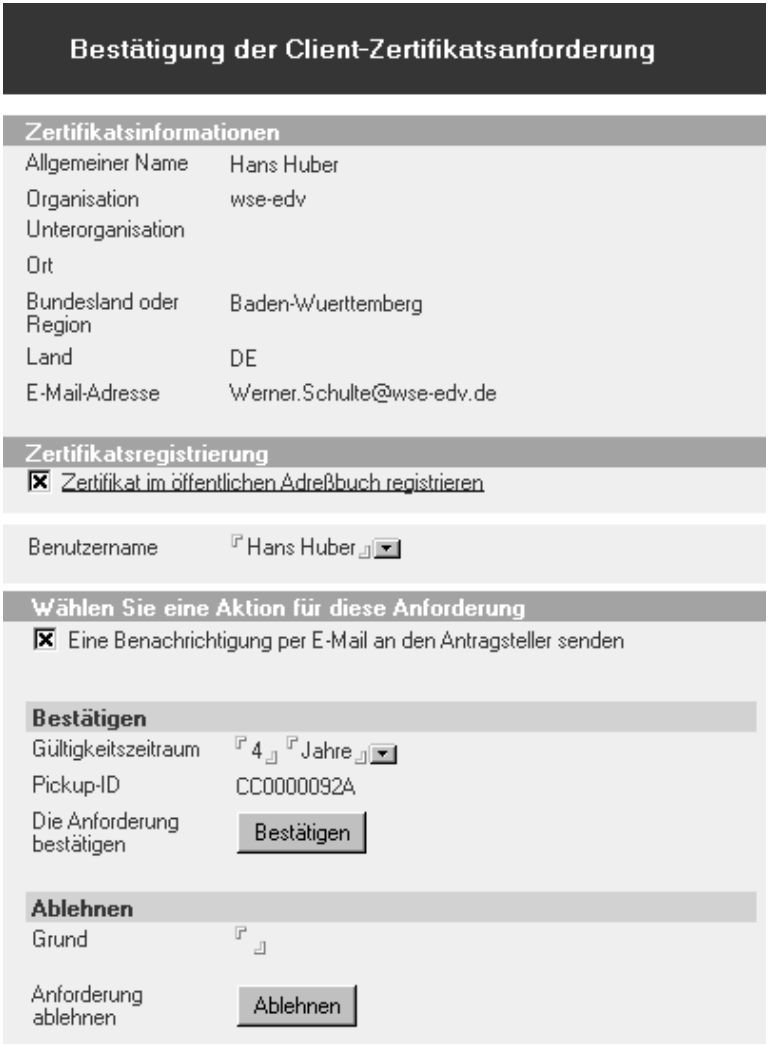
Bestätigung der Zertifikatsanforderung

Der Administrator öffnet nun die Schlüsselring-Datenbank und lässt sich die Liste der Zertifizierungsanforderungen anzeigen.



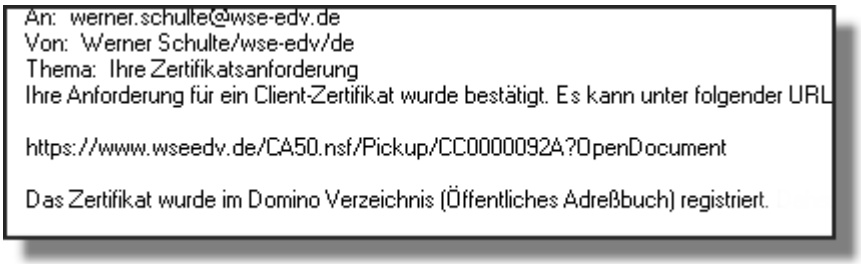
Liste der Zertifizierungsanforderungen

Die neue Anforderung wird geöffnet und vervollständigt. Danach kann sie bestätigt oder abgelehnt werden.



Zertifikatsanforderung bestätigen

Nach der Eingabe des Kennwortes für die Zertifizierungsstelle wird die Zertifizierung durchgeführt und der Benutzer per e-Mail informiert.

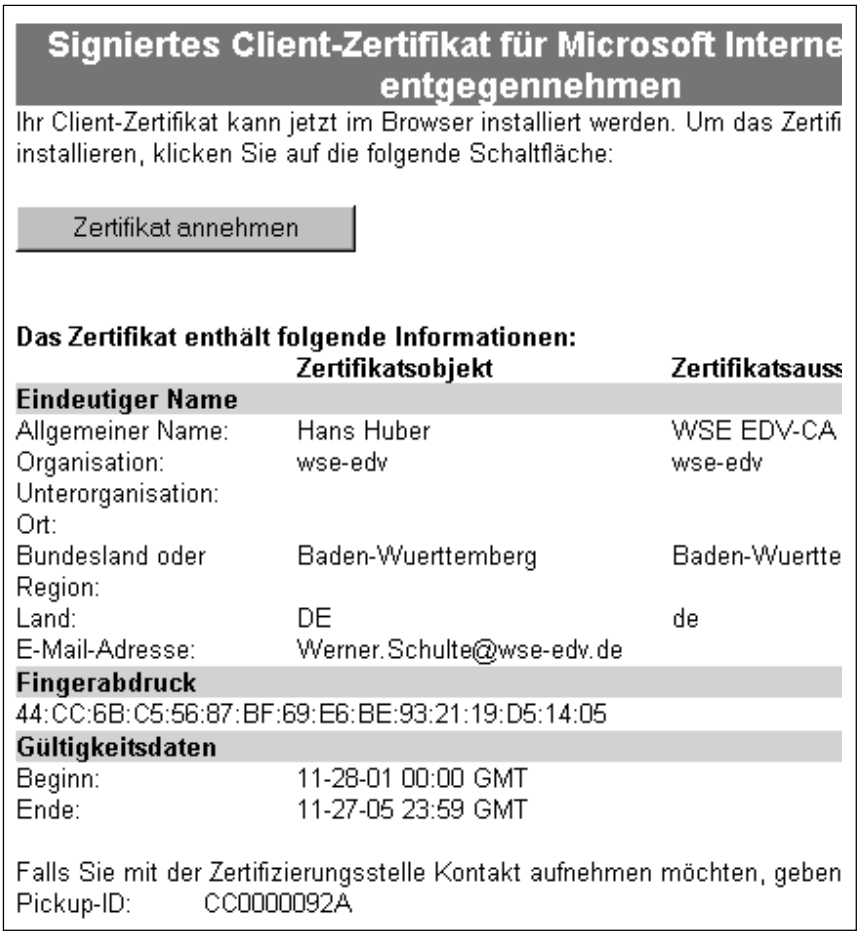

An: werner.schulte@wse-edv.de
Von: Werner Schulte/wse-edv/de
Thema: Ihre Zertifikatsanforderung
Ihre Anforderung für ein Client-Zertifikat wurde bestätigt. Es kann unter folgender URL

https://www.wseedv.de/CA50.nsf/Pickup/CC0000092A?OpenDocument

Das Zertifikat wurde im Domino Verzeichnis (Öffentliches Adreßbuch) registriert.

Bestätigungs-e-Mail

Wird die angegebene URL nachgeschlagen, so öffnet der Browser das Dokument zur Annahme des Zertifikates.



Signiertes Client-Zertifikat für Microsoft Interne entgegennehmen

Ihr Client-Zertifikat kann jetzt im Browser installiert werden. Um das Zertifi installieren, klicken Sie auf die folgende Schaltfläche:

Zertifikat annehmen

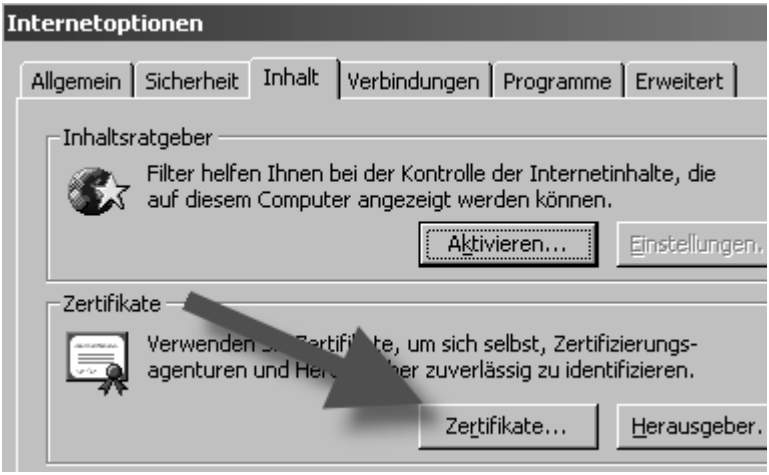
Das Zertifikat enthält folgende Informationen:

	Zertifikatsobjekt	Zertifikatsauss
Eindeutiger Name		
Allgemeiner Name:	Hans Huber	WSE EDV-CA
Organisation:	wse-edv	wse-edv
Unterorganisation:		
Ort:		
Bundesland oder Region:	Baden-Wuerttemberg	Baden-Wuertte
Land:	DE	de
E-Mail-Adresse:	Werner.Schulte@wse-edv.de	
Fingerabdruck		
44:CC:6B:C5:56:87:BF:69:E6:BE:93:21:19:D5:14:05		
Gültigkeitsdaten		
Beginn:	11-28-01 00:00 GMT	
Ende:	11-27-05 23:59 GMT	

Falls Sie mit der Zertifizierungsstelle Kontakt aufnehmen möchten, geben
Pickup-ID: CC0000092A

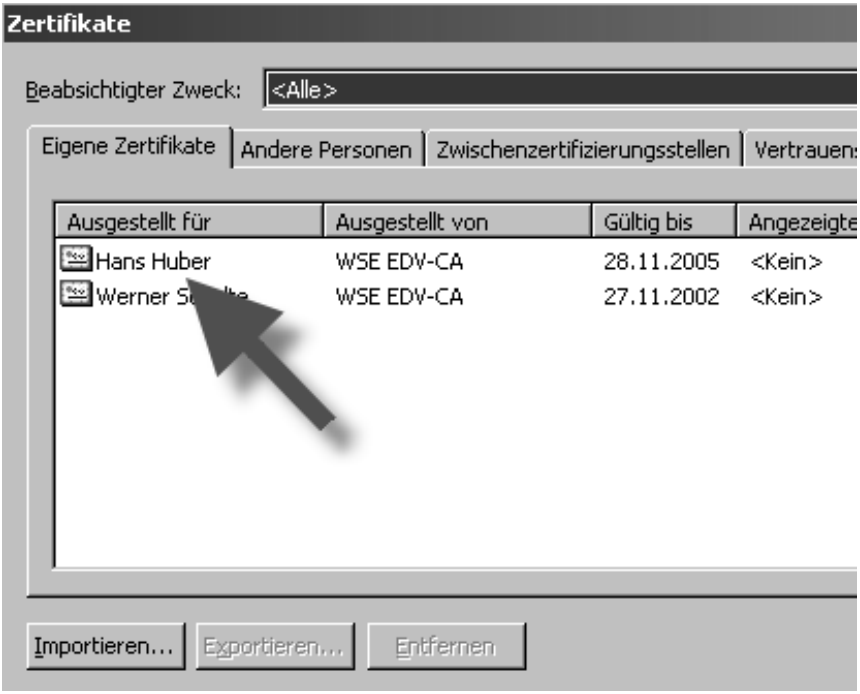
Zertifikat annehmen

Wird das Zertifikat angenommen, so wird es beim Browser als Zertifikat eingetragen. Der Eintrag kann unter „Internetoptionen" im Menü „Extras" angezeigt werden.



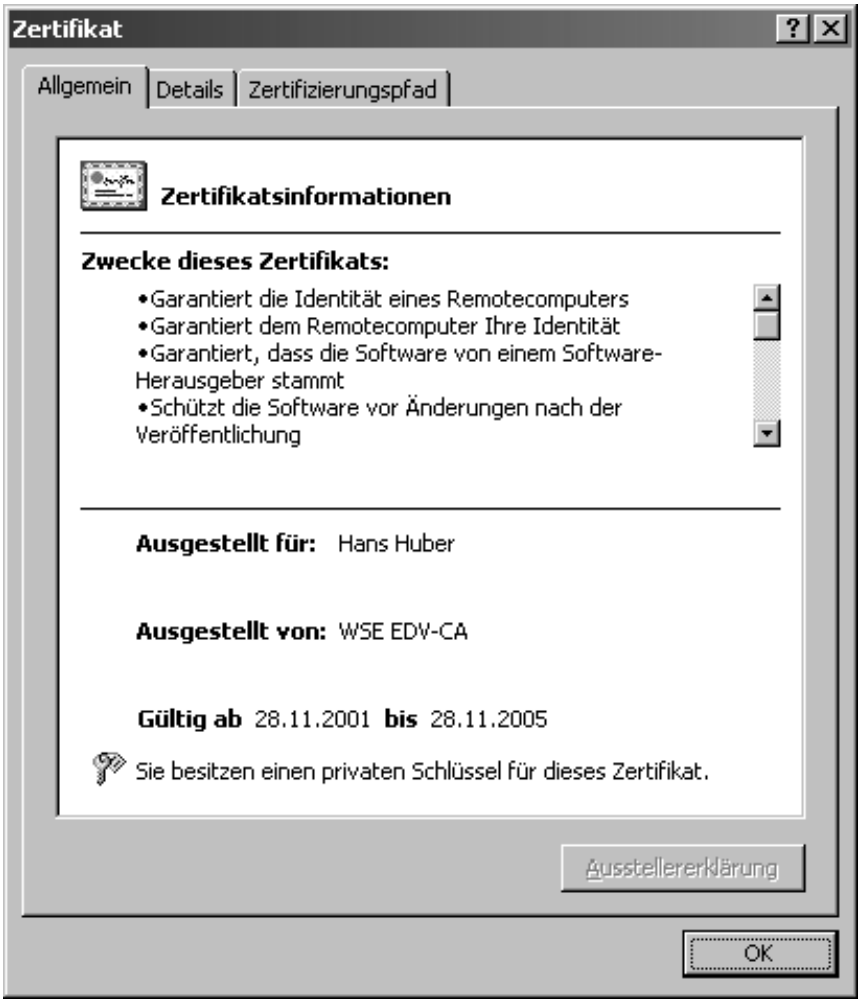
Zertifikate im Internet Explorer

Die Schaltfläche „Zertifikate” öffnet einen Dialog, in dem die Zertifikate aufgeführt sind.



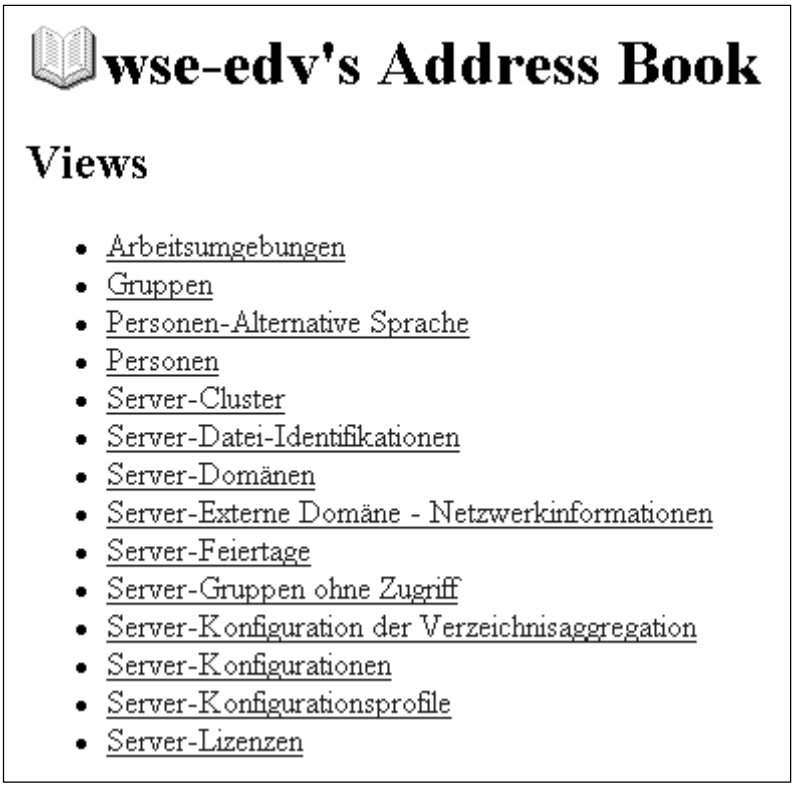
Liste der Zertifikate

Mit Doppelklick werden die detaillierten Angaben zum Zertifikat angezeigt.



Zertifikatsinformationen

Sobald das Zertifikat im Browser installiert ist, kann auf die vorbereitete Datenbank über einen Browser zugegriffen werden.



Datenbankzugriff über den Browser

❶❷❸ Ausführungsschritte:

1. SSL-Verbindung in den Datenbank-Eigenschaften der Datenbank(en), die über Browser verwendet werden sollen, aktivieren.
2. Benutzer im Domino-Verzeichnis anlegen, falls noch nicht vorhanden.
3. Zugriffsrechte der Benutzer in der Zugriffskontrollliste der betroffenen Datenbank(en) festlegen.
4. Zulassungsdatenbank durch den Benutzer über seinen Browser öffnen.
5. Client-Zertifikat mit Hilfe des entsprechenden Formulars durch den Benutzer anfordern.
6. In der Zulassungsdatenbank durch den Administrator die Zertifizierung bestätigen.
7. Durch den Benutzer die URL der Bestätigungs-e-Mail im Browser eingeben.
8. Zertifikat durch den Benutzer annehmen.

❶❷❸

Februar 2002 / 8. EL

Diese Seite ist zur Zeit nicht belegt.

9.6 Richtlinien unter Lotus Domino Release 6

Wer häufig mit der Installation und Betreuung von Notes-Clients zu tun hat, der kennt das Problem: Bei der Installation wird mühsam ein einheitlicher Standard für das Aussehen der Arbeitsoberfläche eingerichtet. Nach einiger Zeit hat dann jeder Benutzer geändert, was ihm gerade passt. Das wäre kein Problem, wenn nicht gerade die Einstellungen gelöscht werden, die unbedingt notwendig sind und auf der anderen Seite Elemente hinzugefügt werden, die nur Verwirrung stiften. Der Benutzerservice kann am Telefon kaum helfen, wenn jeder Arbeitsplatz anders aussieht und jeder Benutzer sich nach eigenem Gutdünken einrichtet.

Mit Release 6 von Lotus Domino werden zur Vereinfachung der Benutzerverwaltung „Richtlinien“ eingeführt, die es dem Administrator ermöglichen, einheitliche Standards für die Bereiche Installation, Anmeldung, Desktop-Gestaltung, Sicherheit und Archivierung festzulegen. Änderungen an diesen Richtlinien werden automatisch bei der nächsten Anmeldung jedes Benutzers auf dessen Client nachvollzogen. Die Zuordnung einer Richtlinie zu einem Benutzer kann entweder über seine hierarchische Zugehörigkeit, über eine Gruppe oder individuell je Benutzer erfolgen. Damit erhält der Domino-Administrator ein Werkzeug zu einer Richtlinien-basierten Systemverwaltung.

Diese Seite ist zur Zeit nicht belegt.

9.6.1 Was ist eine Richtlinie?

Eine Richtlinie ist ein Dokument oder eine Sammlung von Dokumenten, in denen verschiedene Einstellungen, die als Vorgabe dienen sollen, gespeichert werden. Eine Richtlinie stellt eine zentrale Information zur Verfügung, nach der sich alle Notes-Clients richten, die im Geltungsbereich der Richtlinie liegen. Damit können Einstellungen, die für alle Benutzer oder einzelne Gruppen von Benutzern gelten, geändert werden, indem nur das entsprechende Dokument editiert und gespeichert wird. Über die Domino-Prozesse werden die betroffenen Client-Dokumente automatisch angepasst. Die Ausnahme hierzu bilden Einstellungen, die für die Installation eines Clients bzw. die Registrierung eines Benutzers angelegt werden: Änderungen gelten nicht rückwirkend, sondern nur für alle im Anschluss an eine Änderung installierten Notes-Clients bzw. Benutzer.

Die Richtlinien teilen sich auf in die Richtlinien- und in die Einstellungsdokumente. Die Richtliniendokumente regeln den Geltungsbereich in Bezug auf die Benutzer und die Abhängigkeiten zu anderen Richtlinien. Die Einstellungsdokumente enthalten einzelne Einstellungen zu der übergeordneten Richtlinie. Eine Richtlinie kann mehrere Einstellungsdokumente enthalten.

Diese Seite ist zur Zeit nicht belegt.

9.6.2 Die Zuordnung von Richtlinien zu Benutzern

Der Geltungsbereich von Richtlinien kann auf verschiedene Ebenen der Organisationshierarchie bezogen werden. Wenn zum Beispiel eine Organisation aus einer Domäne WSE7 und den Abteilungen Einkauf, Produktion, Vertrieb besteht, dann kann eine Richtlinie für die ganze Domäne WSE7 gelten oder auch nur für eine Abteilung (z.B. */Vertrieb/WSE7). Dabei steht der Stern als Ersatzzeichen für alle Unterorganisationen auf der betroffenen Ebene. Eine Anwendung wäre es z.B., alle Benutzer einer Abteilung als „Roaming User“ anzulegen. Als „Roaming User“ werden die Mitarbeiter bezeichnet, deren Arbeitsplatz nicht in den Büros der Zentrale ist, sondern auf deren Notebook oder auf deren PC im Home-Office mit Notes gearbeitet wird.

Daneben gibt es unabhängige Richtlinien, denen der Benutzer oder eine Benutzergruppe explizit zugewiesen werden müssen. Benutzer und Benutzergruppen können auch verschiedenen Organisationen innerhalb einer Domäne angehören. Diese Art der Richtlinien ist vor allem bei Unternehmen mit flachen Hierarchien sinnvoll oder wenn die Einstellungen nicht der Organisationsstruktur des Unternehmens entsprechen. Wenn z.B. die Einstellungen für „Roaming User“ im Vertrieb nicht einheitlich verwendet werden können, weil die Innen- und Außendienstmitarbeiter in der gleichen Gruppe sind, dann wäre es möglich, eine spezielle Gruppe „Roaming User“ anzulegen und für diese Gruppe eine Richtlinie zu definieren. Damit gelten die Einstellungen für jeden zugeordneten Benutzer unabhängig davon, welchen anderen Gruppen oder organisatorischen Einheiten er angehört.

Diese Seite ist zur Zeit nicht belegt.

9.6.3 Die Standardeinstellungen festlegen

Um Einstellungen für die verschiedenen administrativen Bereiche zu definieren, werden Einstellungsdokumente angelegt und dort die gewünschten Standards, Einstellungen und Konfigurationsparameter hinterlegt.

Die folgenden Arten von Konfigurationsdokumenten enthalten solche Einstellungen:

- **Installationseinstellungen**
  Zur Vereinfachung der Installation und Administration der Lotus Notes-Clients können Festlegungen für die Installation getroffen werden. Sie werden je Arbeitsstation nur einmal, nämlich bei der eigentlichen Installation, verwendet. Zu den Einstellungen, die festgelegt werden können, gehören auch der Internet-Browser, den der Lotus Notes Client verwenden soll, die Parameter für Proxies und die Desktop-Einstellungen. Um die Sicherheit zu erhöhen, kann auch festgelegt werden, welche Applet-Sicherheitseinstellungen befolgt werden müssen.

- **Registrierungseinstellungen**
  Diese Vorgaben werden nur einmal je Benutzer – bei der ersten Registrierung – verwendet. In dem Dokument werden Standardwerte für Kennwörter (Länge, Komplexität) vorgegeben. Weiterhin wird angegeben:

  – welches Format für Internetadressen gilt,

  – ob es sich um einen „Roaming User“ handelt

  – sowie eine Reihe von Vorgaben zur Mail-Datenbank.

- **Desktop-Einstellungen**
  Im Gegensatz zu den Einstellungen, die oben vorgestellt wurden, werden Veränderungen an den Desktop-Einstellungen bei allen Lotus Notes-Clients, für die diese Richtlinie gilt, automatisch nachvollzogen. Die Veränderungen werden beim nächsten Mal, wenn sich der Benutzer anmeldet und die Autorisierung auf dem Lotus Domino-Server erfolgt, entsprechend dem Dokument in den Richtlinien in die Benutzerdaten übertragen. Wenn ein Benutzer eine betroffene Einstellung auf seinem Desktop geändert hatte, wird sie bei der Anmeldung wieder an die Einstellung im Richtliniendokument angepasst. Die Anpassung der Willkommen-Seite gehört ebenfalls zu den Einstellungen, die über die Richtlinien gesteuert werden können.

- **Einstellungen zur Archivierung**
  In diesem Dokument kann eingestellt werden, ob die Archivierung erlaubt ist oder nicht, wohin die Archivierung erfolgen soll und nach welchen einheitlichen Kriterien die Archivierung der Dokumente in den Mail-Datenbanken erfolgen soll.

- **Sicherheitsparameter**
  Zu den Schwerpunkten der Sicherheitsrichtlinien gehört die Verwaltung der ECL (Sicherheitsangaben für die Arbeitsstation). Die Grundlagen bei der Vergabe und Verwaltung von Kennwörtern können festgelegt werden. Und es ist einstellbar, ob das Kennwort für den Lotus Notes-Client und den Zugang über den Internet-Browser synchronisiert werden sollen.

9.6.4 Vererbung von Richtlinien

Das Prinzip der Vererbung, das von der objektorientierten Programmierung her bekannt ist, findet auch bei den Richtlinien Anwendung. Einstellungen, die in einer Richtlinie gemacht wurden, können an eine abgeleitete Richtlinie vererbt werden. Bei hierarchischen Richtlinien findet die Vererbung dabei entlang der Organisationsstruktur des Domino Verzeichnisses statt. Bei den speziellen Richtlinien kann bei der Erstellung eine abgeleitete Richtlinie angelegt werden.

Die Eltern-/Kindbeziehung, die hier implementiert wurde, bietet die Möglichkeit, Richtlinien im Unternehmen einzuführen, in einzelnen Unterbereichen zu verfeinern und trotzdem über die generellen Richtlinien einheitliche Standards zu erzwingen, wenn dies notwendig sein sollte. So kann z.B. in einer Struktur für die Domäne WSE7, die sich in zwei Bereiche aufgliedert (Vertrieb/WSE7 und Einkauf/WSE7) eine hierarchische Richtlinie für WSE7/de angelegt werden. Um abweichende Einstellungen festzulegen, wird für die beiden Bereiche jeweils eine zusätzliche Richtlinie angelegt. Diese Richtlinie hat dann schon automatisch die Voreinstellungen der Richtlinie für WSE7/de. Änderungen und Abweichungen zum Standard werden in den abgeleiteten Richtlinien vorgenommen.

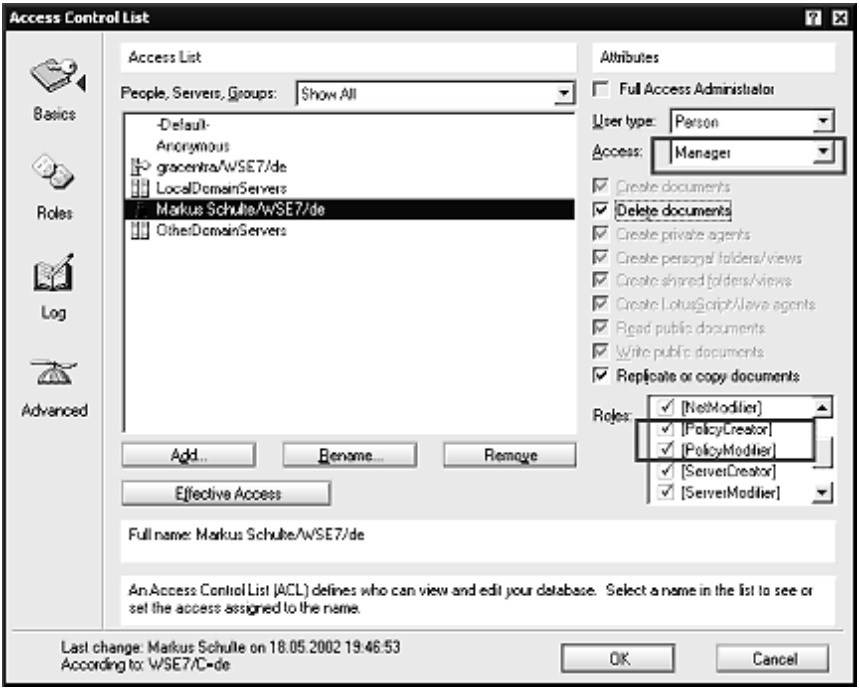
Auf Feldebene kann festgelegt werden, ob die Einstellung vom Elterndokument übernommen und ob die Einstellung für alle abgeleiteten Einstellungen zwingend sein soll.

Diese Seite ist zur Zeit nicht belegt.

9.6.5 Anlegen von Richtlinien

e nach Unternehmensgröße und -struktur ist es sinnvoll, mehrere Richtlinien anzulegen. Dazu wird eine generelle Richtlinie für das ganze Unternehmen erstellt, in der die Einstellungen hinterlegt werden, die für alle Benutzer gelten. Ein Beispiel hierfür wäre die Länge und Komplexität der Kennwörter, die einheitlich für die ganze Domäne geregelt werden sollen. Daneben können bei Bedarf zusätzliche Richtlinien für spezielle Benutzergruppen angelegt werden. Ein weiteres Beispiel aus dem Bereich Sicherheit wäre, dass für mobile Benutzer festgelegt wird, ihre Repliken von Datenbanken grundsätzlich mit der höchsten Verschlüsselung anzulegen. In den folgenden Ausführungen wird von einem solchen Szenario ausgegangen, in dem zunächst eine allgemeine und dann zusätzlich spezifische Richtlinien definiert werden.

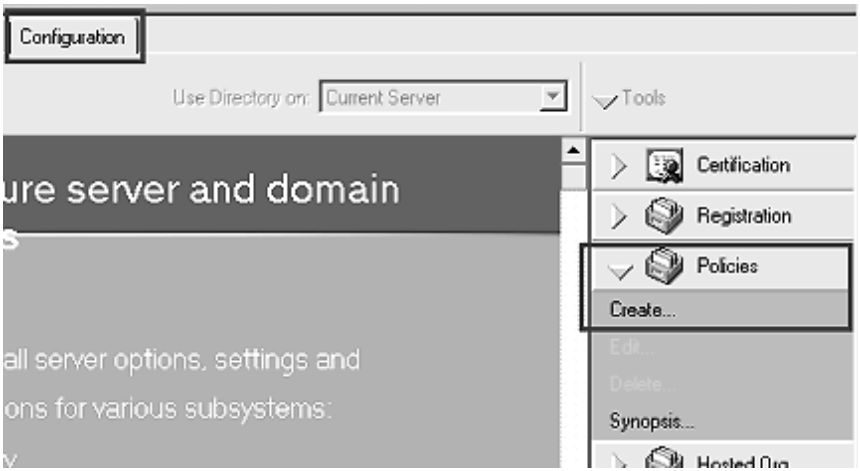
Für Administratoren, die Richtlinien anlegen sollen, muss in der Zugriffskontrollliste des Domino-Verzeichnisses eingetragen sein, dass sie die Rollen „PolicyCreator“ und „PolicyModifier“ haben müssen. Sie müssen außerdem mindestens Editorrechte am Domino-Verzeichnis eingeräumt bekommen.



Einstellungen Zugriffskontrollliste

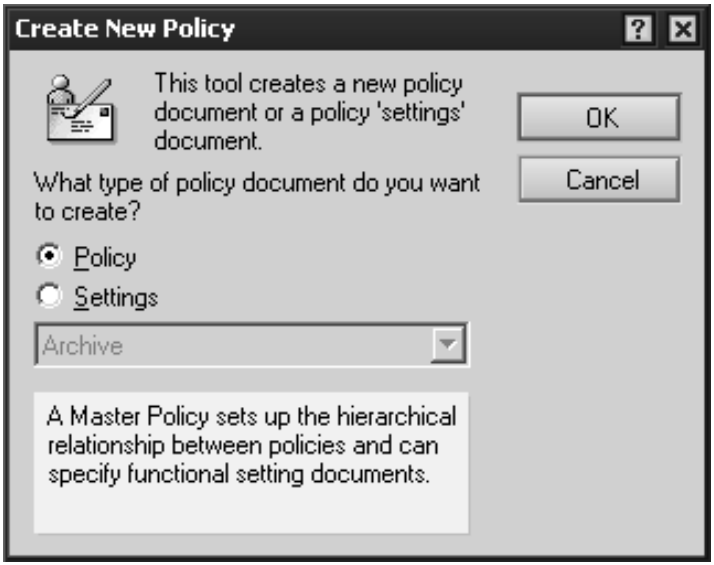
Als Erstes wird über den Administrator-Client das Domino-Verzeichnis ausgewählt, für das Richtlinien angelegt werden sollen. Unter dem Register „Konfiguration“ kann über die Werkzeugleiste im Unterpunkt „Richtlinien“ die Auswahl „Anlegen“ getroffen werden. Die gleiche Auswahl steht über die Menüposition „Konfiguration / Richtlinien / Erstellen“ zur Verfügung.

Auch in der Ansicht „Richtlinien“ kann über die Schaltfläche „Neu“ ein Richtliniendokument erstellt werden.



Richtlinien anlegen

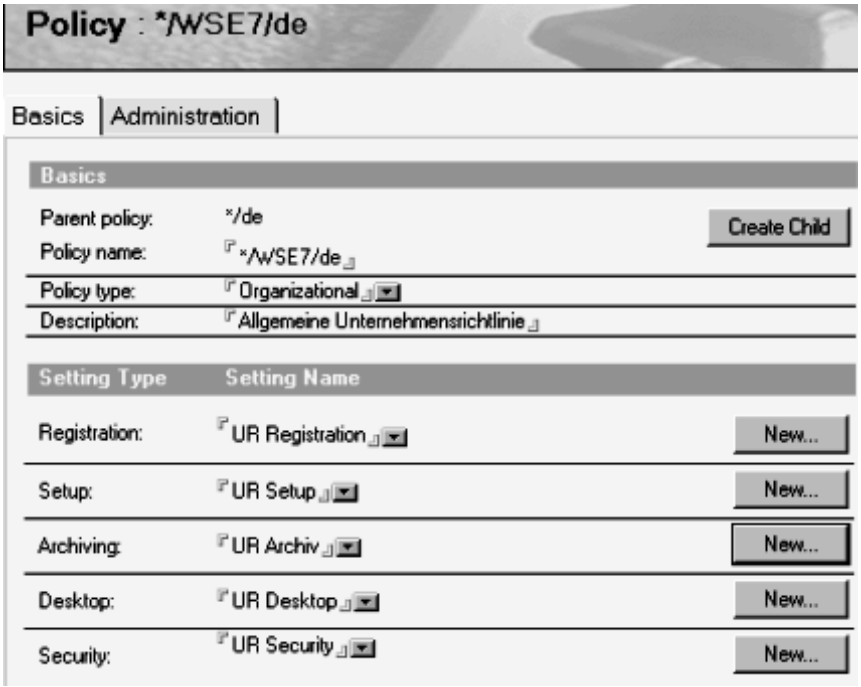
Es erscheint ein Dialogfenster, in dem festgelegt wird, ob Richtlinien oder Einstellungen erstellt werden sollen.



Richtlinie anlegen – Auswahlbox

9.6.5.1 Hierarchische Richtlinien erstellen

Als Erstes wird ein Dokument für eine hierarchische Richtlinie erstellt. In der neuen Richtlinie erfolgt die Zuordnung zur Hierarchie. Dazu wird im ersten Feld der Teil des Hierarchie-Baums angegeben, für den die Richtlinie gelten soll. Alle darunter liegenden Teile der Organisation sind dann ebenfalls eingeschlossen. Im nächsten Feld wird der Typ der Richtlinie ausgewählt: „hierarchisch“. Das folgende Feld kann für eine ausführlichere Beschreibung genutzt werden.



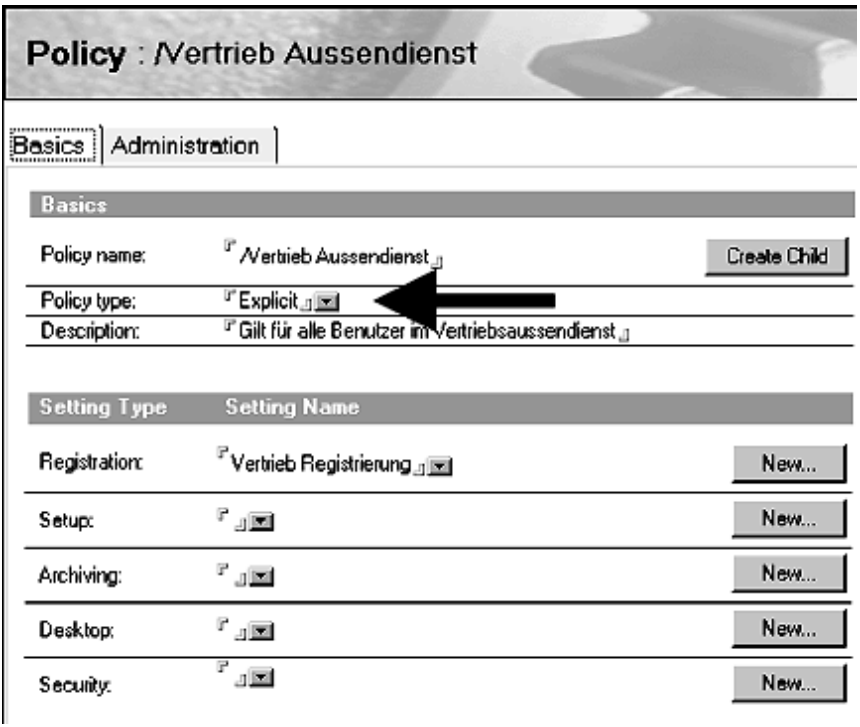
Richtlinie anlegen – hierarchisch

Die Zuordnung der Benutzer zu dem neuen Richtliniendokument erfolgt automatisch über die Position in der Organisationshierarchie.

Die weiteren Auswahlfelder enthalten bereits angelegte Einstellungsdokumente. Mit der Schaltfläche „Neu“ wird ein leeres Dokument angelegt, in dem dann die gewünschten Einstellungen vorgenommen werden können. Für die Richtlinienarten „Registrierung“, „Installation“, „Archivierung“, „Desktop“ und „Sicherheit“ steht jeweils eine Zeile zur Verfügung.

9.6.5.2 Spezifische Richtlinien erstellen

Wenn eine spezifische Richtlinie benötigt wird, ist der Name der Richtlinie frei wählbar. In dem Feld „Typ“ wird „Speziell“ eingetragen. Darunter besteht wieder die Möglichkeit, eine Beschreibung einzugeben. In den folgenden Feldern werden nun die Einstellungsdokumente angelegt und zugeordnet. Während die hierarchischen Richtlinien automatisch über die Organisation auf die Benutzer angewendet werden, müssen spezielle Richtlinien dadurch angewendet werden, dass sie einem Benutzer oder einer Gruppe ausdrücklich zugewiesen werden.



Richtlinie anlegen – Speziell

Diese Zuweisung kann erfolgen:

1. über den Eintrag im Personendokument bzw. gleich bei der Registrierung des Benutzers,

2. über die Zuordnung des Benutzers zu einer Gruppe und der Zuweisung der Richtlinie zu der Gruppe.

Das zweite Verfahren wird auf Grund der vereinfachten Zuordnung bevorzugt eingesetzt werden.

Diese Seite ist zur Zeit nicht belegt.

9.6.6 Einstellungsdokumente

Zur Definition von Einstellungen stehen folgende Dokumentenarten zur Verfügung:

- Archivierungsdokumente
- Desktopdokumente
- Installationsdokumente
- Registrierungsdokumente
- Sicherheitsdokumente

Die verschiedenen Dokumente enthalten Felder, die in Abhängigkeit von der Einstellungsart stehen.

9.6.6.1 Archivdokumente

Das Ziel der Einstellungen für die Archivierung ist es, dem Administrator einen Satz von Regeln an die Hand zu geben, über die Dokumente in den Mail-Datenbanken der Benutzer für die Archivierung ausgewählt und wo sie gespeichert werden. Das Archivierungsdokument wird verwendet, um Einstellungen auf Benutzer-, Gruppen-, Abteilungs- oder Unternehmensebene festzulegen. Die Archivierungseinstellungen gelten jedoch nur für die Mail-Datenbanken der Benutzer. Um andere Datenbanken zu sichern, empfiehlt es sich das Archivierungswerkzeug für Dokumente zu verwenden.

Werden Änderungen am Archivierungsdokument vorgenommen, wirken sich diese automatisch auf alle Benutzer aus, denen diese Richtlinie zugewiesen wurde.

Zum Anlegen des Dokumentes für die Archivierungseinstellungen werden die folgenden Schritte durchgeführt:

❶❷❸ Ausführungsschritte:

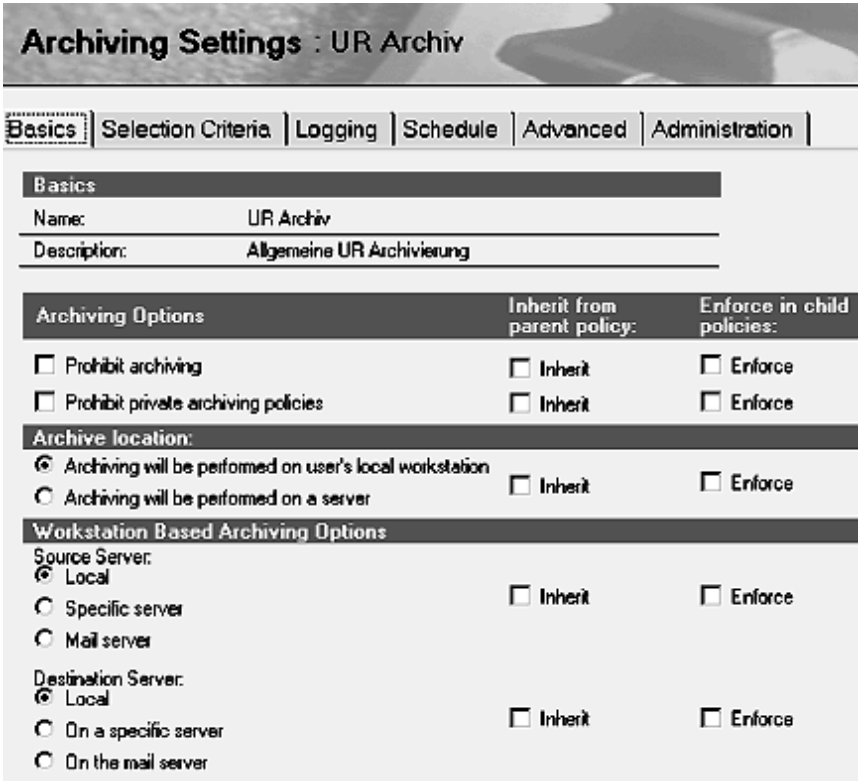
1. Um die Archiveinstellungen verändern oder anlegen zu können, muss der Benutzer Editorrechte und die „PolicyCreator"-Rolle für das Domino-Verzeichnis haben.

2. Vom Domino-Administrator-Client aus wird der Bereich zur Verwaltung von Personen und Gruppen ausgewählt, darunter die Ansicht „Einstellungen".

3. Danach wird die Schaltfläche „Einstellungen hinzufügen" angeklickt und „Desktop" ausgewählt.

4. Wenn ein Dokument für eine abgeleitete Richtlinie angelegt werden soll, wird „Vererben / Ableiten" ausgewählt, damit die Einstellungen des übergeordneten Dokumentes übernommen werden.

❶❷❸



Dokument „Archivierung / Allgemein“

Wichtige Felder im Dokument „Archivierung / Register Allgemein“ sind:

- **Name**
  Name des Dokumentes, in dem die Archiveinstellung gespeichert werden.

- **Beschreibung**
  (wahlfrei) Ausführliche Beschreibung des Archivdokuments.

- **Archivierungsoptionen**
  Es steht zur Auswahl:

  – Archivierung verboten: Die Archivierung kann vom Benutzer nicht aktiviert werden.

  – Private Archivierungseinstellungen verboten: Der Benutzer kann keine eigenen Veränderungen an den Einstellungen vornehmen.

- **Zielort für Archivierung**
  Es kann eine der beiden folgenden Optionen gewählt werden:

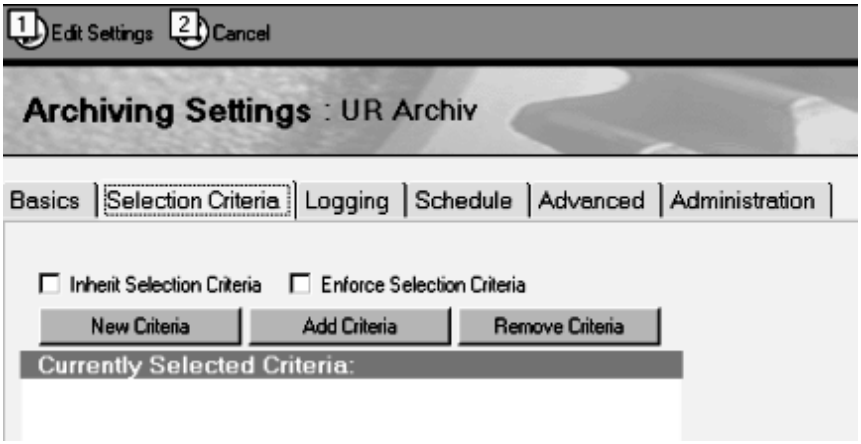
  – Die Speicherung des Archivs erfolgt auf der lokalen Workstation des Benutzers.

  – Der Server wird für die Speicherung der Daten verwendet. Wird diese Option gewählt, müssen die Benutzer die Berechtigung zur Erstellung von Datenbanken auf dem Server haben.

- **Archivierungseinstellungen der Workstation bei lokaler Speicherung**
  Der Ursprungs-Server und der Ziel-Server werden hier angegeben.

- **Archivierungseinstellungen bei Speicherung auf dem Server**
  In dieses Feld werden der Server, auf dem die Speicherung stattfinden soll, und der Mail-Server angegeben.

Die Auswahl der Dokumente, die archiviert werden sollen, erfolgt über ein eigenes Registerblatt mit dem Namen „Auswahlkriterien“:



Dokument „Archivierung / Auswahlkriterien“

Im Register „Auswahlkriterien“ werden die folgenden Felder gefüllt, um festzulegen, welche Dokumente gesichert werden sollen:

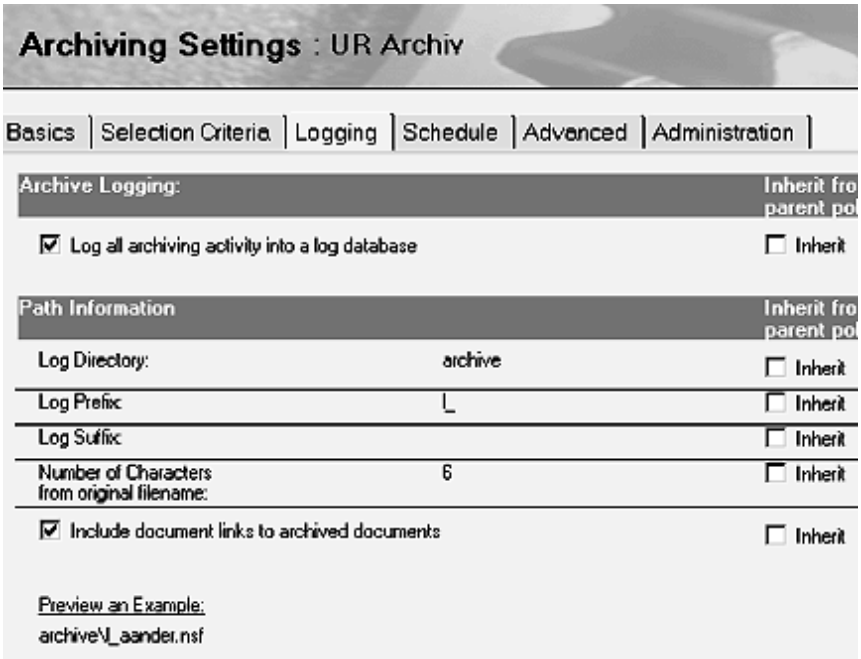
- **Neues Kriterium**
  Auf diese Schaltfläche klicken, um neue Kriterien für die Auswahl der zu archivierenden Dokumente anzulegen.

- **Kriterium hinzufügen**
  Klicken und dann aus der Liste der verfügbaren Kriterien eines auswählen, das für die Archivierung verwendet werden soll.

- **Kriterium löschen**
  Klicken. Dann kann ein zugeordnetes Kriterium gelöscht werden.

- **Kriterien anzeigen**
  Zeigt die momentan zugeordneten Kriterien an.

Über das Register „Protokollierung“ wird konfiguriert, welche Aufzeichnungen über die Archivierung erstellt werden.



Dokument „Archivierung / Protokollierung“

Felder

- **Alle Archivierungsaktivitäten protokollieren**
  Standardmäßig aktiviert. Vervollständigen Sie den Pfad für die Speicherung, wenn Sie eine neue Datenbank verwenden wollen. Wenn nicht protokolliert werden soll, wird diese Option deaktiviert.

- **Verzeichnis für Protokoll**
  Hier wird ein Pfad eingetragen, für den Fall dass der Standardpfad (C:\notes\data\archive) nicht verwendet werden soll.

- **Präfix für Protokolldatenbanken**
  Das Standardpräfix ist „l_“. Hier kann auch eine andere Buchstabenkombination eingegeben werden.

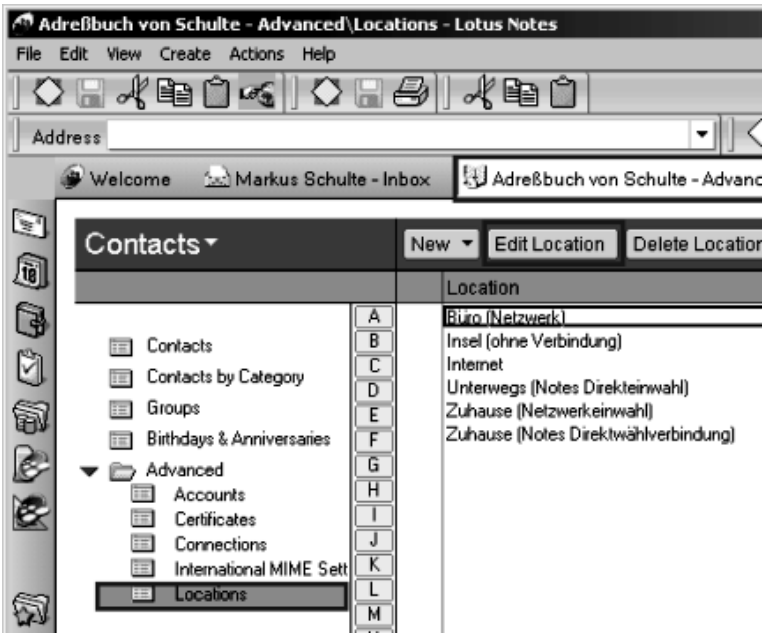
- **Suffix**
  Das Standardsuffix kann hier geändert werden.

- **Anzahl der Zeichen vom Originaldatenbanknamen**
  Anzahl der Zeichen, die vom Originalnamen der Datenbank im Namen der Protokolldatenbanken wieder verwendet werden sollen.

- **Links auf Originaldokumente einfügen**
  Standardmäßig aktiviert.

9.6.6.2 Desktop-Dokumente

Die Einstellungen für den Desktop steuern die Arbeitsumgebung des Benutzers. Viele der Einstellungen, die hier verändert werden können, sind auch im Setup-Dokument enthalten und können dort voreingestellt werden. Der Unterschied liegt darin, dass das Desktop-Dokument für die laufende Administration verwendet wird, während das Setup-Dokument nur einmal bei der Registrierung des Benutzers verwendet wird. Veränderung und Modifikationen der Richtlinien aus dem ursprünglichen Setup-Dokument werden nur über die Einstellungen des Desktop-Dokuments ermöglicht. Benutzer erhalten ein Update auf Ihre Einstellungen, wenn sie sich bei Ihrem Heimat-Server, der in der Arbeitsumgebung angegeben wird, anmelden.



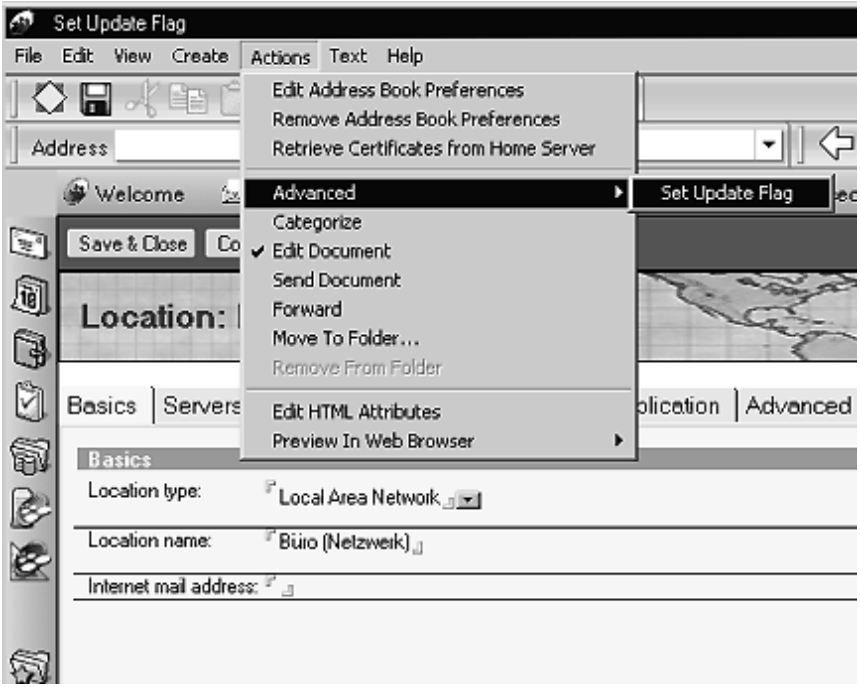
Arbeitsumgebung bearbeiten

Einstellungen im Desktop-Dokument können verändert oder hinzugefügt, aber nicht gelöscht werden. Das bedeutet konkret, dass ein Verweis auf eine Datenbank in die Lesezeichenleiste eines Benutzers eingefügt werden kann, aber dass er später nicht wieder entfernt werden kann.

In Fällen, wo es nicht gewünscht ist, dass Einstellungen im Desktop-Dokument durch Änderungen von Richtlinien beeinflusst werden, können Benutzer dies durch eine entsprechende Einstellung in der Arbeitsumgebung festlegen.

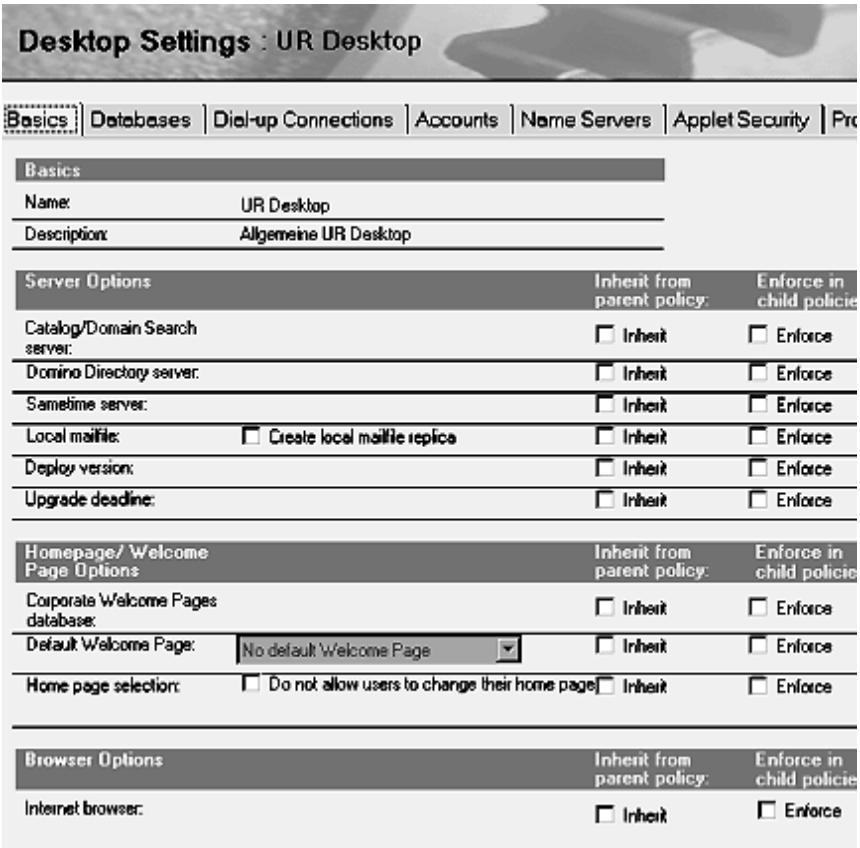
Um Veränderungen durch das Desktop-Dokument an den Desktop-Einstellungen zu verhindern, wird die Arbeitsumgebung zur Bearbeitung (Persönliches Namens- und Adressbuch / Erweitert /Arbeitsumgebungen / Arbeitsumgebung bearbeiten) geöffnet.

Dann wird über „Aktionen / Erweitert" das Update-Flag eingestellt.



Arbeitsumgebung Update-Flag setzen

Die Angaben im Register „Allgemein“ des Desktop-Dokumentes ähneln denen des Archivdokumentes.



Dokument „Desktop / Allgemein“

Zum Anlegen des Dokumentes für die Desktop-Einstellungen werden die folgenden Schritte durchgeführt:

❶❷❸ Ausführungsschritte:

1. Um Desktop-Einstellungen verändern oder anlegen zu können, muss der Benutzer Editorrechte für das Domino-Verzeichnis und die „PolicyCreator"-Rolle haben.

2. Vom Administrator-Client aus wird der Bereich zur Verwaltung von Personen und Gruppen ausgewählt, darunter die Ansicht „Einstellungen".

3. Die Schaltfläche „Einstellungen hinzufügen" wird angeklickt und dann „Desktop" ausgewählt.

4. Wenn ein Dokument für eine abgeleitete Richtlinie angelegt werden soll, wird „Vererben/Ableiten" ausgewählt, damit die Einstellungen des übergeordneten Dokumentes übernommen werden. Bei jeder Einstellung kann festgelegt werden, ob sie in abgeleiteten Richtlinien erzwungen werden soll oder nicht.

5. Im Bereich „Allgemein" alle gewünschten Felder ausfüllen.

6. Das Register "Datenbank" auswählen und die Felder bei Bedarf ausfüllen. Hier können die folgenden Informationen für alle Passthru- und für alle anderen Remote-Server erfasst werden:

   - Server-Name

- Ländercode (z.B. +49 für Deutschland)
- Vorwahl (z.B. 0711 für Stuttgart)
- Telefonnummer des Anschlusses (123456)

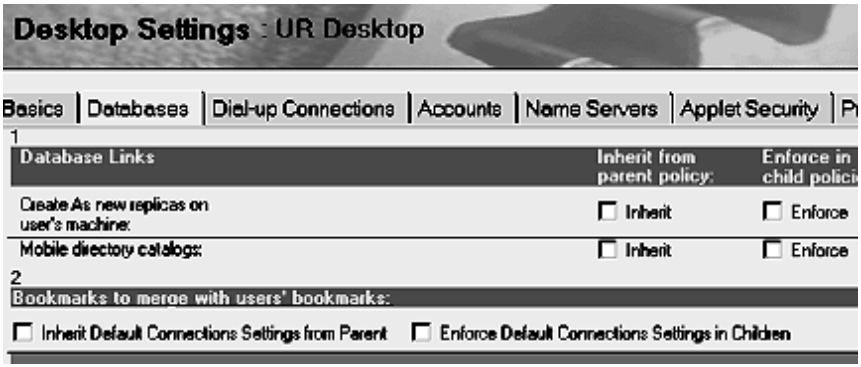
7. Das Register “Konto” enthält folgende Felder:
   - Name
   - Server-Adressen
   - Protokoll
   - SSL-Verbindungen zu Internet-Servern, die von Benutzern erreichbar sein sollen
8. Übrige Registerblätter ausfüllen
9. Speichern und verlassen des Dokuments.

Einige der Dokumentfelder im Desktop-Dokument werden hier noch einmal näher beschrieben.

Felder für das Dokument „Desktop" im Register „Allgemein":

- **Name**
  Wählen Sie hier einen möglichst aussagekräftigen Namen, unter dem Sie die Richtlinie wiederfinden können. Dieser Name wird in der Ansicht der Richtlinien angezeigt.
- **Beschreibung**
  (wahlfrei) Hier kann eine weitere ergänzende Beschreibung der Desktop-Einstellungen eingegeben werden.
- **Verzeichnis-Server**
  Wählen Sie hier den Domino-Server, der das zu verwendende Domino-Verzeichnis enthält.
- **Sametime-Server**
  Geben Sie hier den Namen des zu verwendenden Sametime-Servers ein.
- **Lokale Mail-Datenbank**
  Hier kann der Name der Mail-Datenbank eingegeben werden, wenn eine Kopie der Mail-Datenbank auf dem lokalen PC gespeichert werden soll.
- **Software-Version**
  Wenn der automatische Software-Update für die Lotus Notes-Clients verwendet werden soll, kann hier die Software-Version eingestellt werden.

- **Übergangszeit**
  In diesem Feld kann eingetragen werden, wann die Übergangszeit für die Aktualisierung der vorgegebenen Software-Version ablaufen soll. Danach muss der Benutzer die Aktualisierung durchführen.
- **Unternehmensweite Datenbank für „Welcome"-Seiten**
  Hier kann der Name einer Datenbank angegeben werden, in der einheitliche Begrüßungsseiten für das gesamte Unternehmen gespeichert werden können.
- **Standard-"Welcome"–Seite**
  Der Name der Seite, die Benutzer vorgeschlagen bekommen, wenn Sie ihren Lotus Notes-Client installieren.
- **Homepage-Vorgabe**
  Hier kann verhindert werden, dass die Benutzer sich eine eigene Homepage einstellen.
- **Internet-Browser**
  Voreinstellung für den zu verwendenden Internet-Browser.
- **Seiten öffnen**
  (wahlfrei) Wenn Notes als Internet-Browser verwendet wird, muss hier eingestellt werden, wo der Prozess laufen soll, der die gewünschten Seiten aus dem Internet abruft.



Dokument „Desktop / Datenbank“

Felder des Registers „Datenbank“:

Felder

- **Als neue Replik auf dem PC des Benutzers anlegen**
  Für jede Datenbank, für die automatisch eine Replik angelegt werden soll, wird hier eine Verknüpfung eingefügt.
- **Mobile Domino-Verzeichnisse**
  Tragen Sie hier Links von allen Domino-Verzeichnissen ein, die auf den lokalen PCs verfügbar sein sollen.
- **Lesezeichen, die mit den lokalen Lesezeichen des Benutzers zusammengeführt werden sollen**
  Hier können Links, URLs oder Verzeichnisse als Namen oder per „Drag and Drop“ eingefügt werden, die dann mit den lokalen Lesezeichen des Benutzers zusammengefügt werden.

Hier noch ein Auswahl von Feldern, die bei den entsprechenden übrigen Reitern gefüllt werden können:

- **Namens-Server**
  Hier können die Namen von sekundären TCP/IP- und NDS-Domino-Namens-Servern angegeben werden.
- **Applet-Sicherheit**
  Festlegen der „Trusted Hosts“ in einer Organisation und einstellen der Netzwerkadressen aller vertrauenswürdigen und nicht vertrauenswürdigen Hosts.
- **Proxies**
  Falls Standard-Proxies verwendet werden sollen, können hier deren Adressen eingetragen werden.
- **MIME**
  Hier kann ausgewählt werden, welches Format e-Mail-Nachrichten haben soll, die ins Internet verteilt werden:
  – Notes-Richtext-Format
  – MIME
- **Präferenzen**
  Die grundlegenden Präferenzen für den Desktop, die Internationalen Einstellungen, die e-Mail- und News-Konfiguration.
- **Administration**
  Wählen Sie hier die Namen der Eigentümer und der Administratoren für dieses Einstellungsdokument.

9.6.6.3 Registrierungsdokumente

Die Registrierung von Benutzern kann erheblich vereinfacht werden, indem Richtliniendokumente für sie angelegt werden. Wenn eine hierarchische Richtlinie existiert, bevor ein Benutzer registriert wird, dann werden die Felder in den entsprechenden Masken bereits voreingestellt. Außerdem können während der Registrierung noch spezielle Richtlinien zugewiesen werden, die dann ebenfalls die Voreinstellungen in den Feldern vornehmen. Statt bei jedem Benutzer die Einstellungen vorzunehmen, kann so der Registrierungsprozess vereinheitlicht und standardisiert werden.

❶❷❸ Ausführungsschritte:

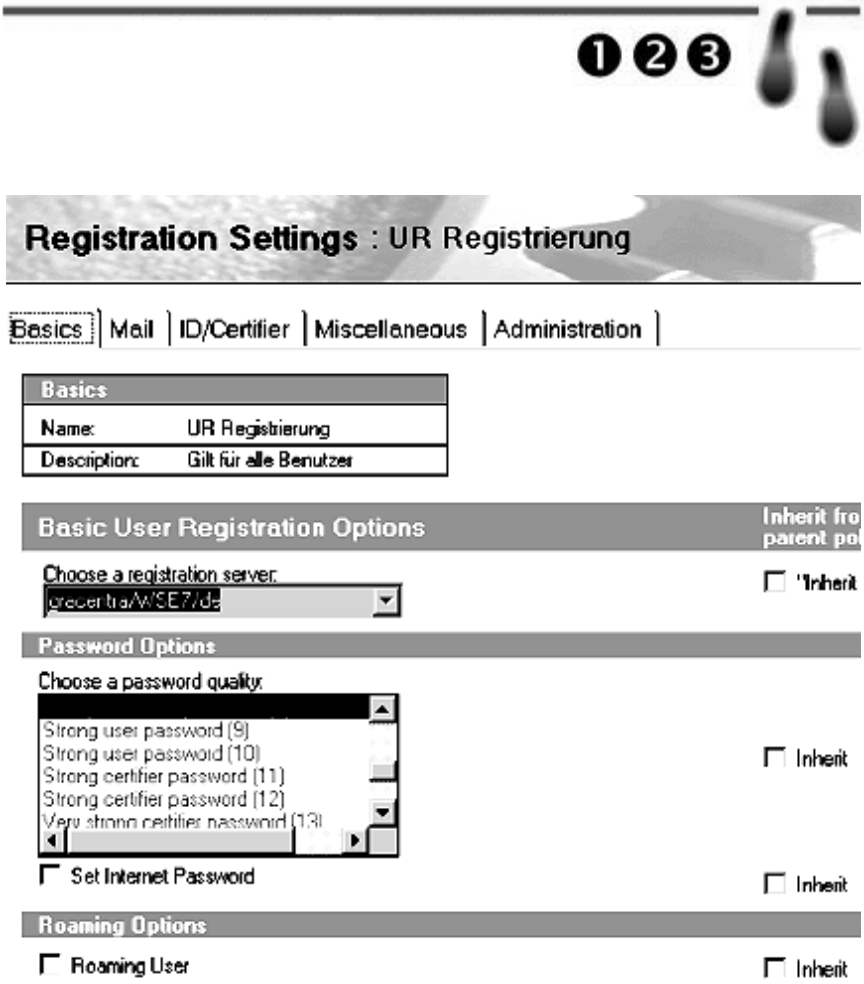
1. Wer ein Einstellungsdokument für Registrierungsrichtlinien anlegen will, muss mindestens Editorrechte in der Zugriffskontrollliste des Domino-Verzeichnisses haben. Außerdem muss ihm die Rolle „PolicyCreator“ zugewiesen sein.

2. Im Administrator-Client das Register „Personen und Gruppen“ und dann die Ansicht „Einstellungen“ auswählen.

3. Die Schaltfläche „Einstellung hinzufügen“ anklicken und dann „Registrieren“ auswählen.

4. Falls ein Einstellungsdokument für eine abgeleitete Richtlinie erstellt werden soll, wird die Auswahl „Ableiten“ eingesetzt, um die Einstellungen des Elternobjektes zu übernehmen.

5. Übrige Felder ausfüllen und das Dokument speichern.



Dokument „Registrierung / Allgemein“

Felder

- **Name**
  Hier wird ein möglichst beschreibender Name für die Benutzer gewählt, für die diese Registereinstellungen gelten sollen. Der Name wird dann in der Ansicht für die Richtlinien angezeigt.

- **Beschreibung**
  Bei Bedarf kann hier noch eine zusätzliche, ausführlichere Beschreibung erstellt werden.

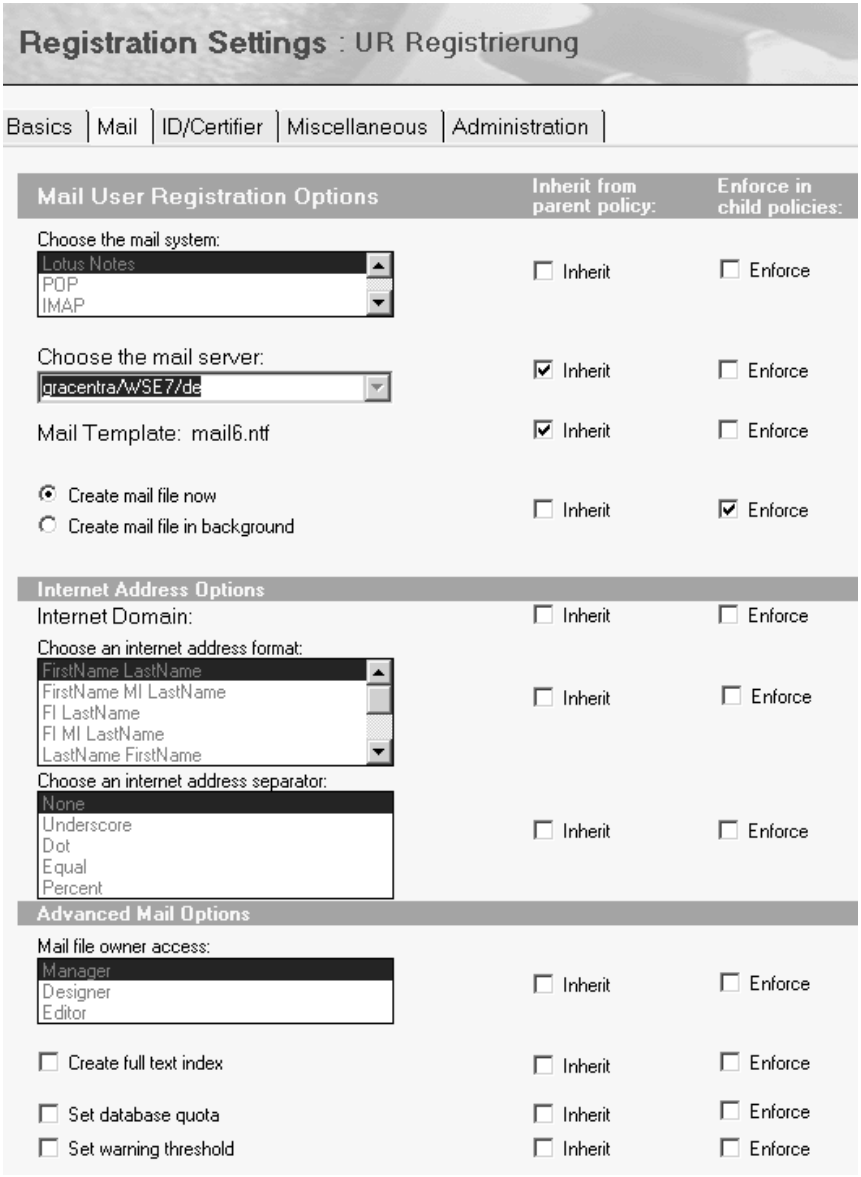
- **Registrierungs-Server**
  Hier wird der Server angegeben, mit dem der Lotus Notes-Client Verbindung aufnimmt, um die bei der Registrierung notwendigen Aufgaben auszuführen. Er kann aus der Liste der verfügbaren Registrierungs-Server ausgewählt werden.

- **Wählen Sie eine Mindestqualität für Kennwörter**
  Sicherheitsebene, die für Kennwörter gewünscht wird. Es werden verschiedene Kombinationen von Komplexität und Anzahl zu verwendender Zeichen zur Verfügung gestellt.

  Hinweis:
  Diese Einstellungen werden nur für die Registrierung und bei der ersten Anmeldung verwendet. Nachdem sich der Benutzer beim Server identifiziert hat, gelten die Standardsicherheitseinstellungen.

- **Internet-Kennwort festlegen**
  Wenn die Benutzer über einen Internet-Browser zugreifen können, wird hier ein Internet-Kennwort vorgegeben. Das Kennwort wird im Personendokument abgelegt.

- **Roaming User**
  Voreinstellung für Benutzer, den das Roaming erlaubt werden soll. Alle notwendigen Vorgaben können hier durchgeführt werden.
- **Mail-Server für Roaming User**
  Gilt nur für Roaming User: Wenn diese Auswahl aktiviert wird, erfolgt die Speicherung der Informationen über Roaming und die entsprechenden Profile auf dem gleichen Server, auf dem auch die Mail-Datenbank des Benutzers gespeichert wird. Ansonsten kann im darauf folgenden Feld der Server eingestellt werden, wo die Daten gehalten werden sollen.
- **Optionen für die Erstellung der notwendigen Dateien für Roaming User**
  Gilt nur für Roaming User: Entweder werden die Dateien für den Benutzer sofort erstellt, wenn der Benutzer registriert wird, oder die Dateien werden im Hintergrund angelegt. Die Erstellung erfolgt dann beim nächsten Mal, wenn der Administrationsprozess auf dem Server gestartet wird.
- **Optionen für Reorganisation**
  Gilt nur für Roaming User:
  – Entweder wird nie reorganisiert, es wird keine Reorganisation der Dateien des Roaming Benutzers durchgeführt.
  – Reorganisation alle N-Tage, hier wird die Anzahl der Tage eingegeben, die zwischen den Reorganisationsläufen liegen soll (0 - 365).
  – Reorganisation beim Beenden des Lotus Notes-Clients, hier wird die Reorganisation jedes Mal durchgeführt, wenn der Lotus Notes-Client beendet wird.



Dokument „Registrierung / Mail“

Felder

- **Wählen Sie das Mail-System**
  Hier wird eingestellt, welches Mail-System in Ihrer Organisation verwendet wird. Wenn im Unternehmen e-Mails über HTTP zur Verfügung gestellt werden, kann eine der drei folgenden Möglichkeiten gewählt werden:
  – Lotus Notes: benötigt eine Lotus Notes ID
  – POP3
  – IMAP
- **Auswahl des Mail-Servers**
  Einstellen des Mail-Servers. Wenn DOLS im Unternehmen verwendet wird, muss dies ein DOLS-Server sein.
- **Mail-Schablone**
  Hier empfiehlt sich die Verwendung der Standardschablone „mail6.ntf“. Falls Erweiterungen der Mail-Schablone vorgenommen wurden, kann hier der Name der geänderten Schablone eingetragen werden.
- **Mail-Datenbank sofort erstellen**
  Bestimmt den Zeitpunkt, zu dem die Mail-Datenbank erstellt wird: sofort oder beim nächsten Lauf des Administrationsprozesses.
- **Internet-Domäne**
  Diese Domäne wird an die Internet-Adresse des Benutzers angehängt. Dies ist die Internet-Domäne und nicht die Notes Domäne.
- **Internet-Adressformat**
  Adressformat für e-Mails, die ins Internet gesendet werden.

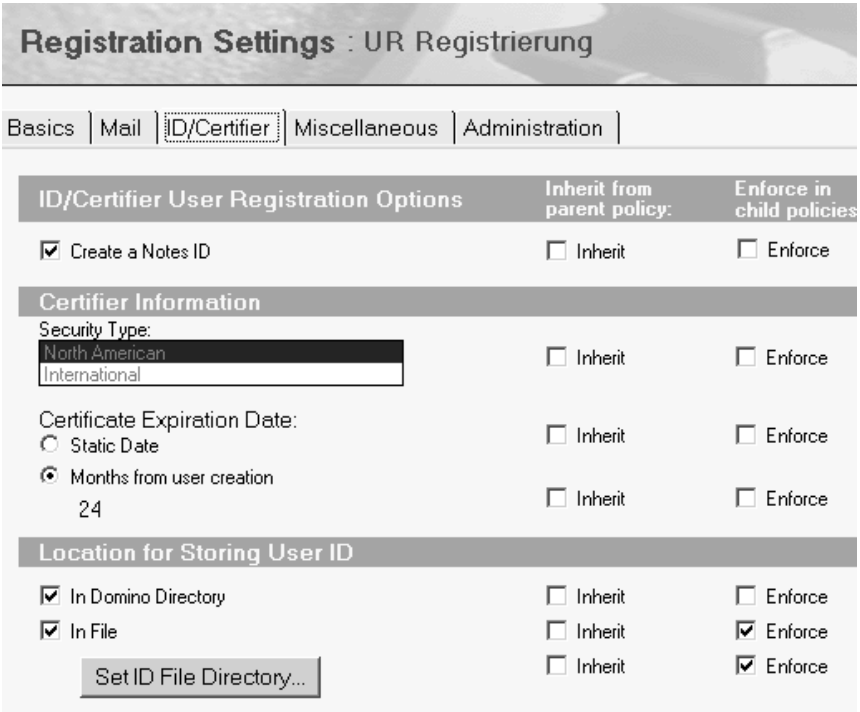
- **Internet-Adress-Separator**
  Zeichen, das bei Internet-e-Mails im Namensteil des Benutzers als Trennzeichen verwendet werden soll.

- **Maildatenbank: Zugriff für Eigentümer**
  Hier wird die Zugriffsebene ausgewählt, die der Eigentümer der Mail-Datenbank bekommt. Es wird empfohlen, hier maximal „Editor" zu verwenden. Dadurch hat der Benutzer die Möglichkeit, e-Mails, aber nicht die komplette Datenbank zu löschen.

- **Volltext-Index anlegbar**
  (wahlfrei) Falls der Benutzer die Möglichkeit bekommen soll, einen Volltext-Index für seine Datenbank zu erstellen, wird diese Auswahl angeklickt. Diese Auswahl steht auch für POP3 und IMAP zur Verfügung.

- **Maximale Datenbankgröße festlegen**
  Hier wird voreingestellt, ob für Mail-Datenbanken eine maximale Größe festgelegt werden soll. Die Größe der Datenbank wird in Megabyte angegeben.

- **Grenze für Vorwarnung festlegen**
  Wenn diese Auswahl angeklickt wird, erhält der Benutzer eine Warnung, dass die maximale Größe der Datenbank demnächst erreicht sein wird. Die Grenze, wann vorher die Warnung erfolgt, wird in Megabyte angegeben.

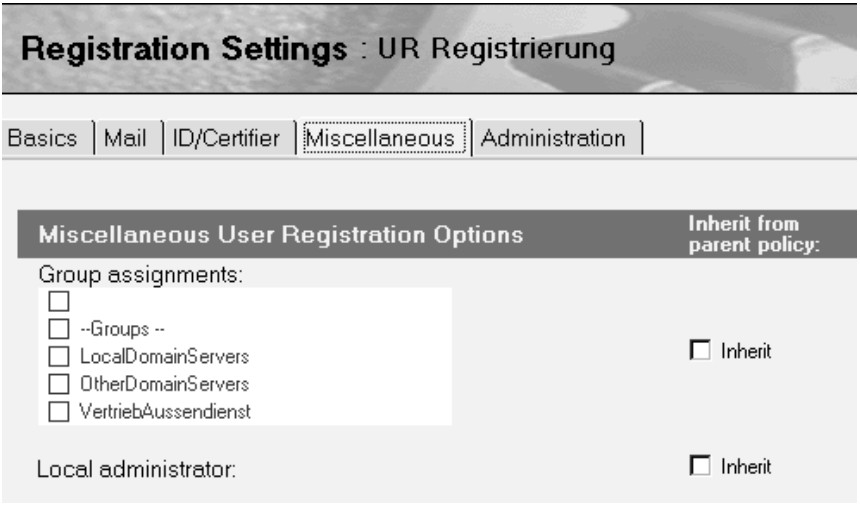


Dokument „Registrierung / ID“

Felder

- **Erstellen einer Notes-ID**
  Auswählen, wenn während der Registrierung eine Notes-ID erstellt werden soll.
- **Sicherheitstyp**
  Entweder „Nordamerika“ oder „International“. Hier wird angegeben, wie viele Bits für den Schlüssel bei der Verschlüsselung eingesetzt werden sollen.

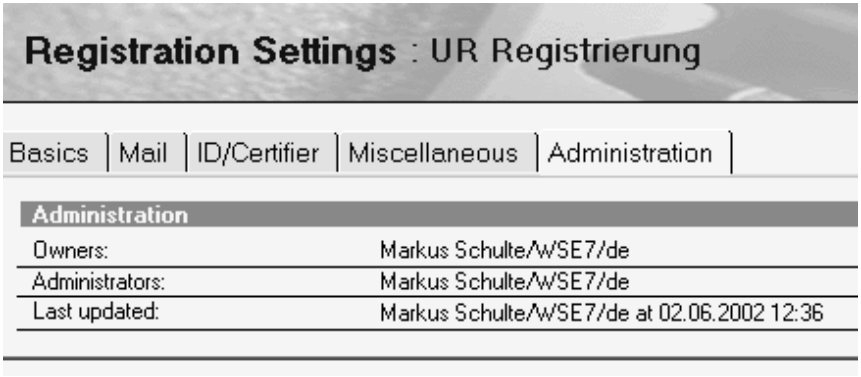
- **Ablaufdatum des erstellten Zertifikates**
  Wählen Sie unter den folgenden Optionen aus:
  - **Festes Datum**:
    Ein festes Standarddatum wird vorgegeben, kann aber geändert werden.
  - **Monate ab Erstellung der Benutzerkennung**:
    Als Standard werden hier 24 Monate vorgeschlagen, aber jeder andere Wert ist ebenfalls möglich.
- **Speicherort für die Benutzer-ID**
  Eine oder beide der folgenden Optionen kann ausgewählt werden. Wenn beide gewählt werden, erfolgt die Speicherung an beiden Orten:
  - **Im Domino-Verzeichnis**
    Die ID des Benutzers wird im Personendokument im Domino-Verzeichnis gespeichert.
  - **In einer Datei**
    „ID-Datei speichern“ anklicken, um den Pfad auszuwählen, unter dem IDs gespeichert werden sollen.



Dokument "Registrierung / Verschiedenes"

Felder

- **Gruppenzugehörigkeit**
  Hier wird eine Gruppe ausgewählt, zu der alle Benutzer gehören sollen, die mit dieser Registrierungsrichtlinie erstellt werden. Sollen die Benutzer keiner Gruppe zugewiesen werden, oder wenn sie nicht alle der gleichen Gruppe zugehören, bleibt das Feld leer.
- **Lokaler Administrator**
  Name des Administrators



Dokument „Registrierung / Administration“

Felder

- **Eigner**
  Der Eigentümer der Registrierungsrichtlinie kann aus der Liste ausgewählt werden.
- **Administratoren**
  Auch die zuständigen Administratoren können aus einer Liste ausgewählt werden.
- **Letzte Aktualisierung**
  Hier wird vom System eingetragen, wann die Richtlinie zuletzt aktualisiert wurde.

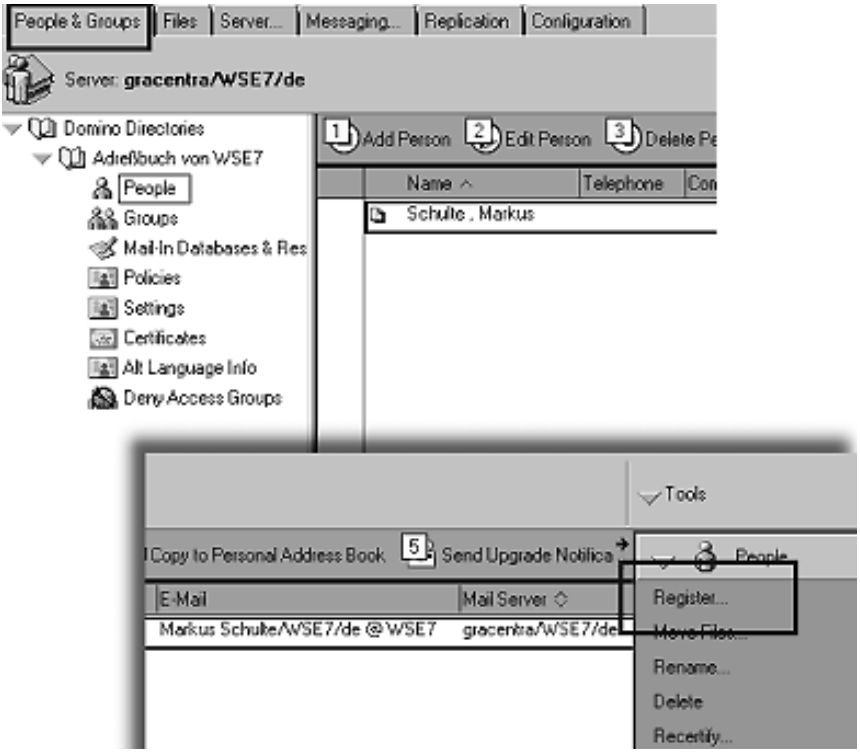
Diese Seite ist zur Zeit nicht belegt.

9.6.7 Zuordnung von Richtlinien

Wie schon erwähnt, gibt es drei verschiedene Möglichkeiten, eine spezifische Richtlinie zuzuordnen:

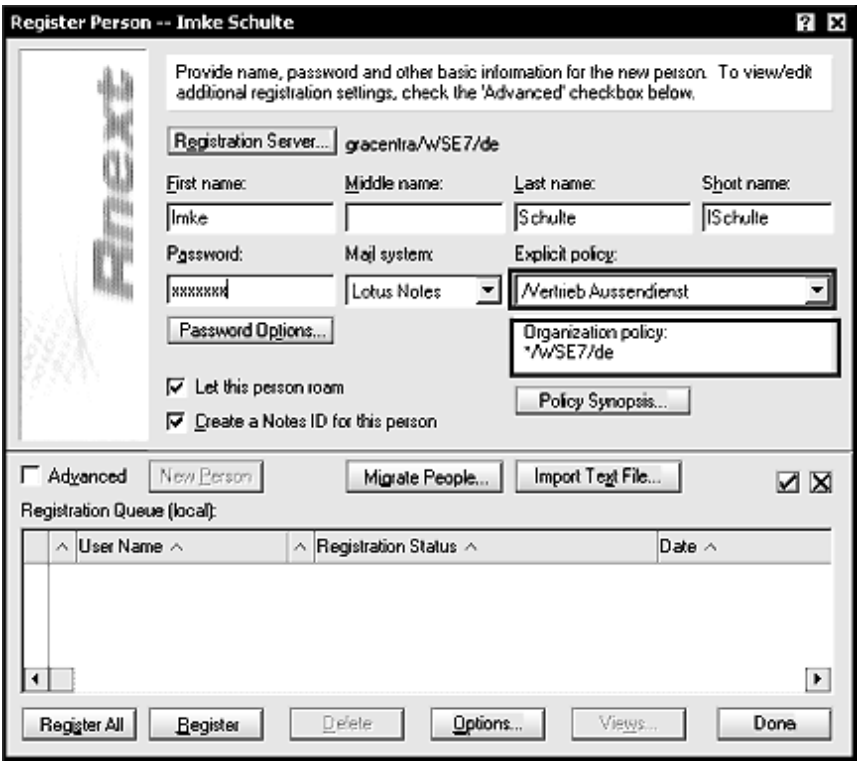
9.6.7.1 Zuordnung bei der Registrierung

Die Registrierung eines Benutzers wird über den Administrator-Client durchgeführt. Im Bereich „Personen und Gruppen“ wird der Menüpunkt „Register / Registrierung“ verwendet.



Zuordnung bei der Registrierung

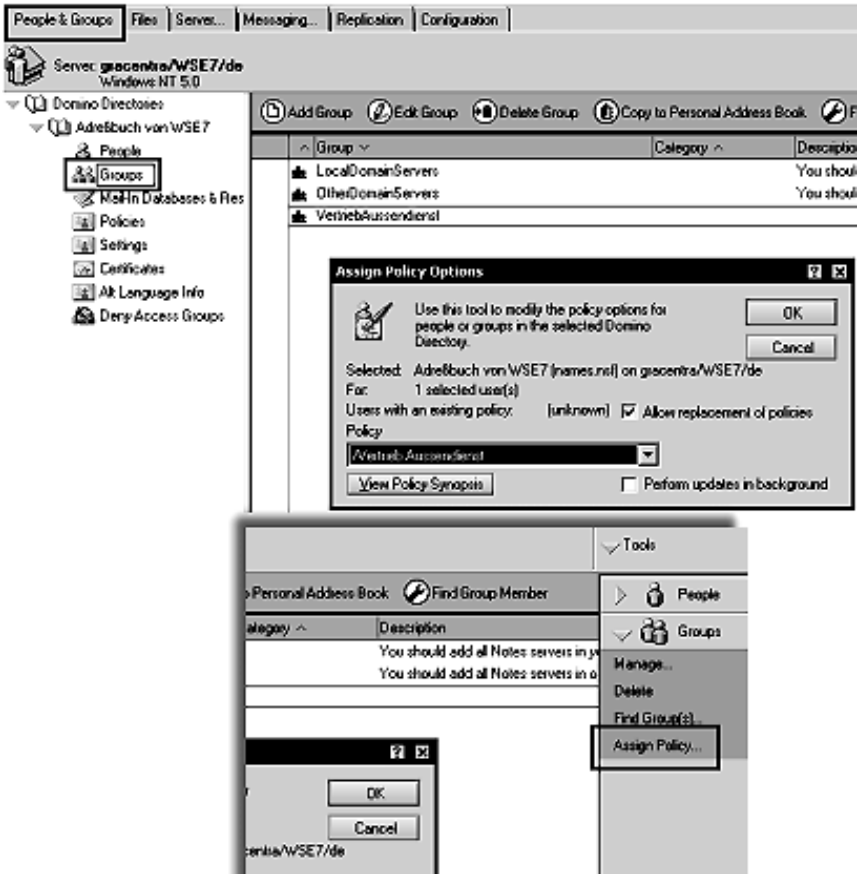
Nachdem der Benutzer zu der Zertifizierer-ID gewechselt hat, erscheint die gewohnte Abfragemaske zum Registrieren von neuen Benutzern.



R*egistrierung / Personen*

Dabei ist sofort zu erkennen, dass für den neuen Benutzer eine hierarchische Richtlinie existiert. Zusätzlich kann in dem Feld „spezielle Richtlinie“ eine weitere Richtlinie festgelegt werden.

Wenn auf die Schaltfläche „Übersicht Richtlinien“ geklickt wird, kann ein Bericht über die schon geltenden Richtlinien und deren Einstellungsdokumente aufgerufen werden.



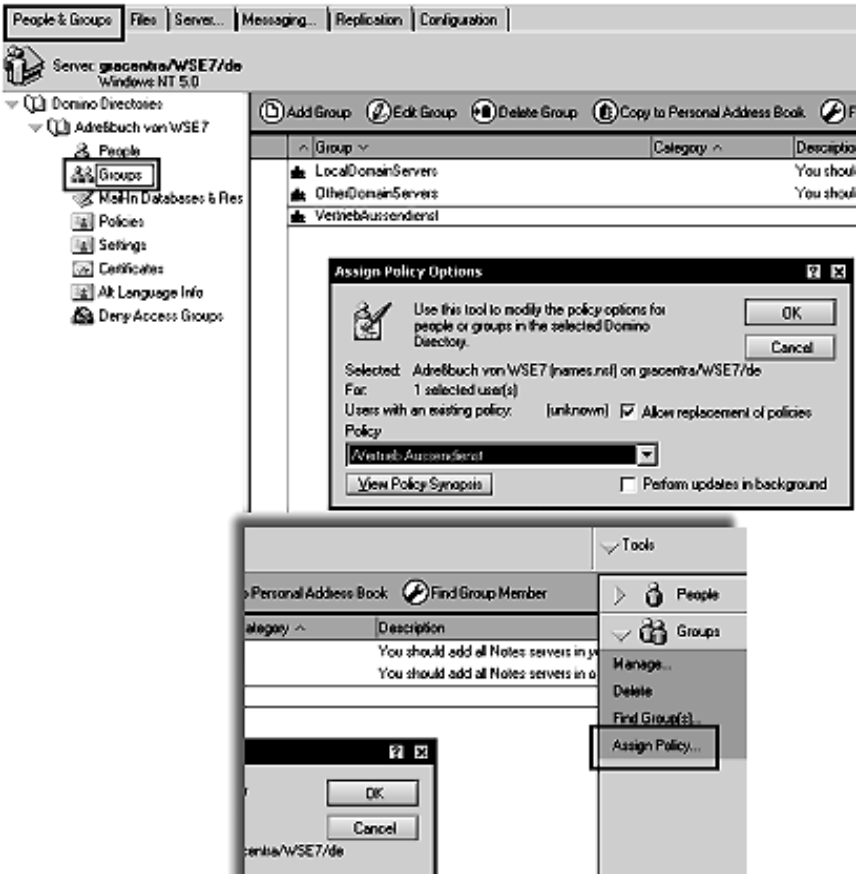
Bericht Richtlinien

9.6.7.2 Zuordnung über das Personendokument

Bei bestehenden Benutzern kann die Zuordnung einer Richtlinie zu einer Person in das Feld „Richtlinie“ eingetragen werden. Die Person wird über den Lotus Administrator-Client geöffnet. Im Bereich „Administration“ befindet sich in der rechten Spalte unter „Richtlinien-Management“ das Feld „Zugewiesene Richtlinie“.

9.6.7.3 Zuordnung über eine Gruppe

Zur Vereinfachung der Verwaltung kann die Zuordnung auch über Benutzergruppen gesteuert werden. Die Zuweisung erfolgt genau wie bei den Personen über den Administrator-Client im Bereich „Personen / Gruppen“. Hier wird eine Gruppe ausgewählt und über die Werkzeugleiste eine Richtlinie der Gruppe zugeteilt. Ein Feld – wie in dem Personendokument – gibt es allerdings nicht.



Zuordnung über eine Gruppe

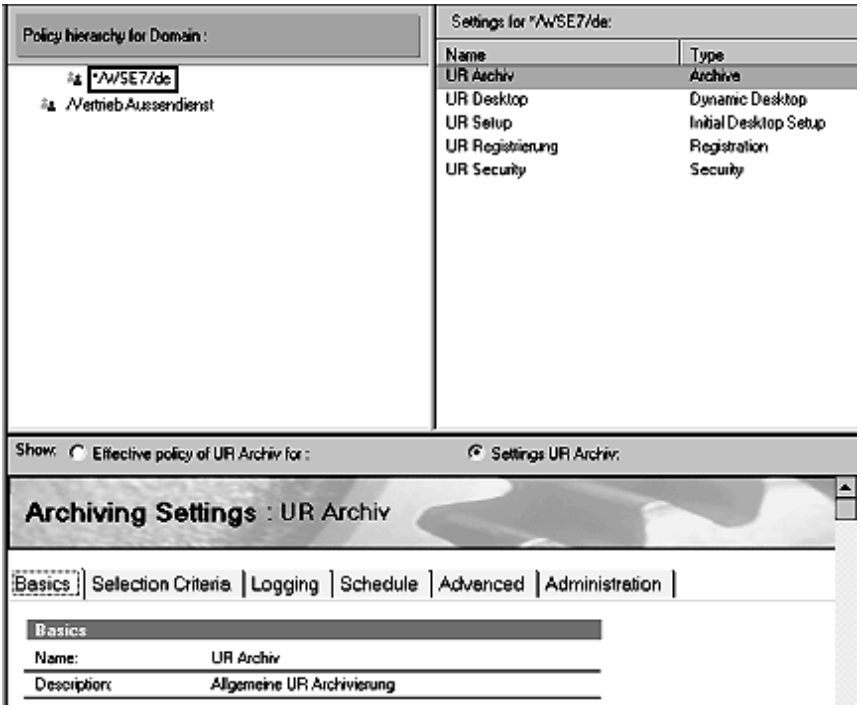
Diese Seite ist zur Zeit nicht belegt.

9.6.8 Welche Richtlinie ist gültig

Jede Hierarchiestufe kann eine eigene Richtlinie haben. Dadurch können für eine Person mehrere Richtlinien gleichzeitig gültig sein. Um zu ermitteln, welche Richtlinie gültig ist, muss der Hierarchie-Baum von oben nach unten durchlaufen werden. Es kann beispielsweise erlaubt werden, dass in einer abgeleiteten Richtlinie eine Einstellung verändert werden darf. Dann gilt die Einstellung der abgeleiteten Richtlinie. Wenn im hierarchisch höheren Dokument angegeben wurde, dass die vorgenommene Einstellung nicht verändert werden darf, dann gilt immer die Einstellung aus dieser Richtlinie. Um zu ermitteln, welche Richtlinie die gültige für den gewählten Benutzer ist, gibt es zwei Werkzeuge:

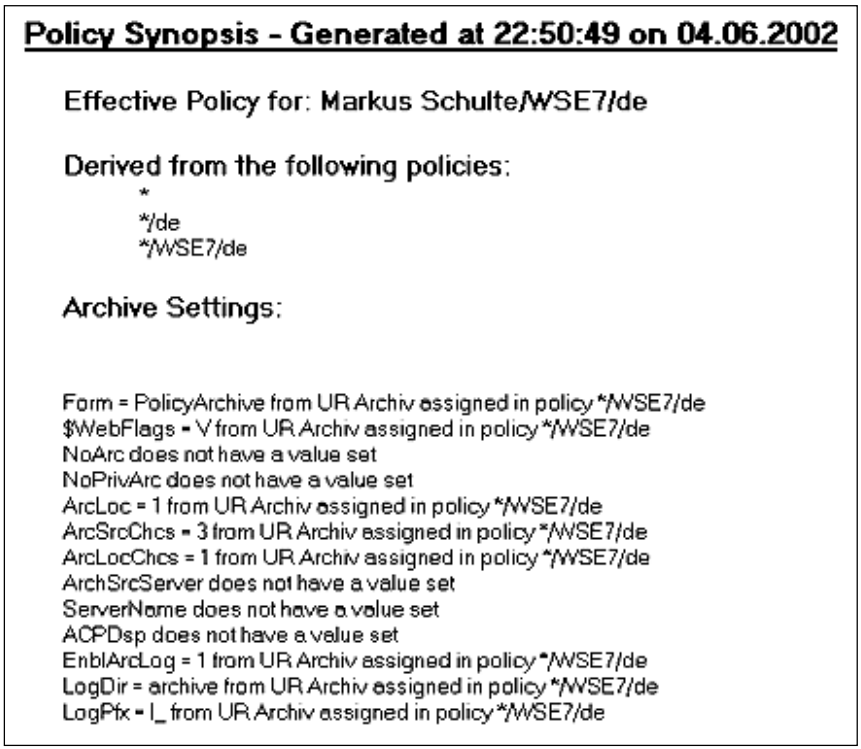
- die Richtlinienansicht im Administrator-Client
- und die Richtlinienzusammenfassung.

In der Richtlinienansicht werden die Richtlinienhierarchie und die dazugehörigen Einstellungsdokumente in der Übersicht gezeigt.



Richtlinienansicht

Die Ansicht kann nach Hierarchiestufen oder nach Einstellungsdokumenten angezeigt werden. Mit der Richtlinienzusammenfassung kann ein Bericht ausgegeben werden, der über die Hierarchie und alle effektiven Einstellungen Auskunft gibt.



Policy Synopsis - Generated at 22:50:49 on 04.06.2002

Effective Policy for: Markus Schulte/WSE7/de

Derived from the following policies:

*
*/de
*/WSE7/de

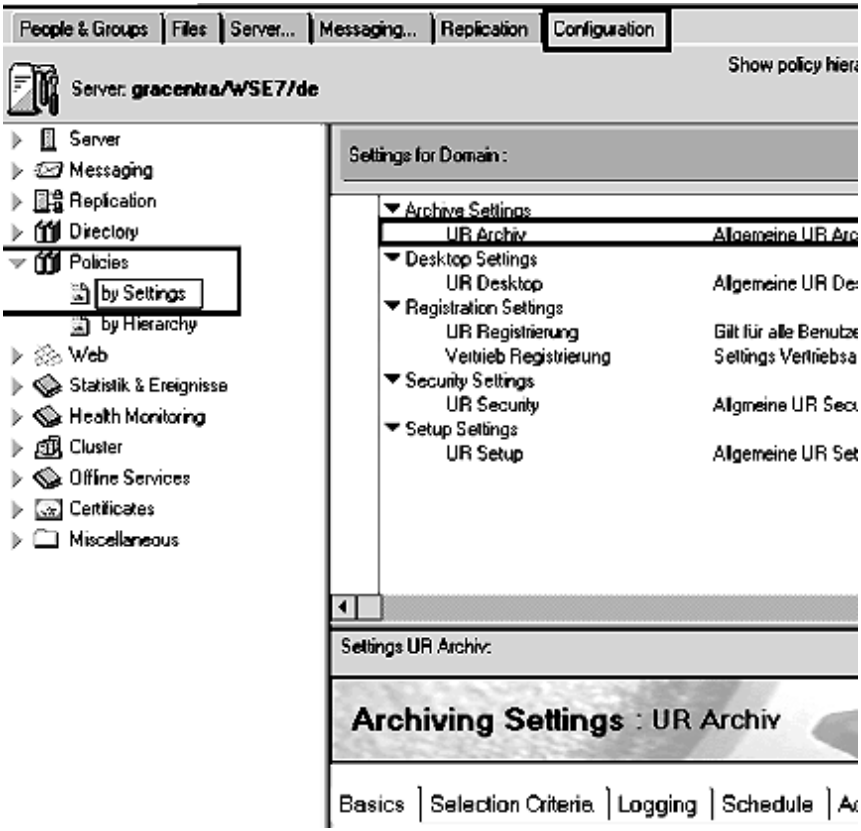
Archive Settings:

Form = PolicyArchive from UR Archiv assigned in policy */WSE7/de
$WebFlags = V from UR Archiv assigned in policy */WSE7/de
NoArc does not have a value set
NoPrivArc does not have a value set
ArcLoc = 1 from UR Archiv assigned in policy */WSE7/de
ArcSrcChcs = 3 from UR Archiv assigned in policy */WSE7/de
ArcLocChcs = 1 from UR Archiv assigned in policy */WSE7/de
ArchSrcServer does not have a value set
ServerName does not have a value set
ACPDsp does not have a value set
EnblArcLog = 1 from UR Archiv assigned in policy */WSE7/de
LogDir = archive from UR Archiv assigned in policy */WSE7/de
LogPfx = l_ from UR Archiv assigned in policy */WSE7/de

Richtlinienzusammenfassung

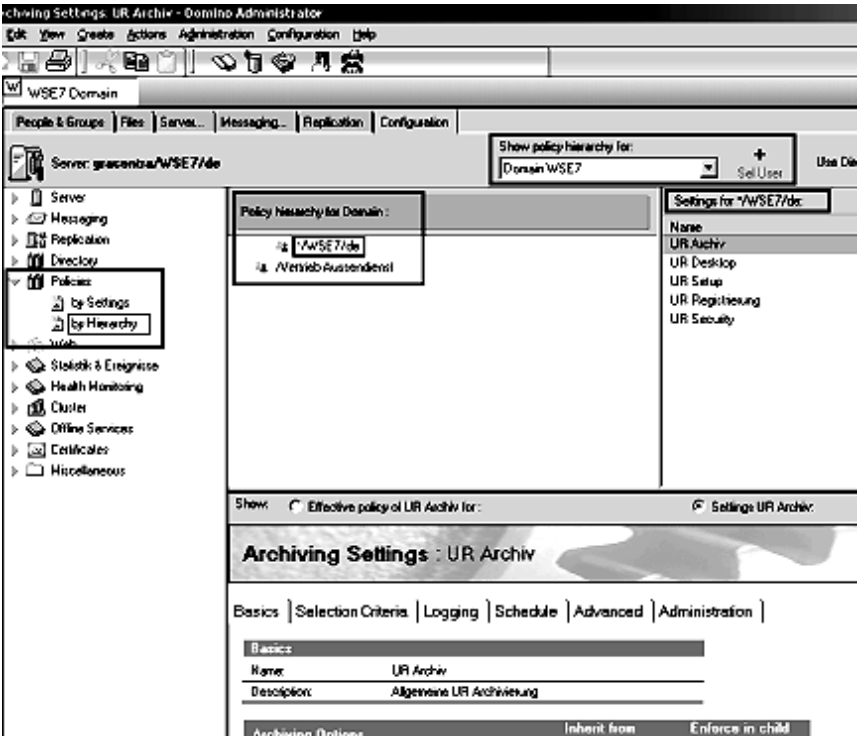
9.6.8.1 Die Richtlinienansicht

Um in die Richtlinienansicht zu gelangen, muss im Administrator-Client der Bereich „Konfiguration“ ausgewählt werden. Im linken Auswahlfenster wird zunächst auf “Richtlinie” geklickt. Hier befinden sich dann die schon erwähnten zwei Ansichten: nach Einstellungsdokument und nach Hierarchiestufe. In der Ansicht nach „Einstellungen“ befinden sich in dem linken oberen Fenster alle Einstellungsdokumente der aktuellen Domäne. Im Fenster rechts daneben wird der entsprechende Hierarchie-Baum der Richtliniendokumente angezeigt, in denen das ausgewählte Einstellungsdokument verwendet wird. Im unteren Fenster wird die Maske mit dem Einstellungsdokument angezeigt. Änderungen an dem betreffenden Dokument können direkt ausgeführt werden.



Richtlinienansicht – nach Einstellungen

Wenn die Ansicht nach Hierarchie ausgewählt wird, wechselt der Inhalt der beiden oberen Fenster. Je nach gewählter Richtlinie im linken Fenster befinden sich im rechten Fenster die dazugehörigen Einstellungsdokumente. Zusätzlich kann über die beiden Fenster ausgewählt werden, ob die Richtlinien für einen bestimmten Benutzer angezeigt werden sollen.



Richtlinienansicht – nach Hierarchie

9.6.8.2 Die Richtlinienzusammenfassung

Um genau zu ermitteln, welche Richtlinien für einen Benutzer gelten, kann die Richtlinienzusammenfassung erstellt werden. Sie wird in Form eines Berichtes erstellt, in dem zu erkennen ist, wie die Hierarchie aufgebaut und welche Einstellungen in den jeweiligen Dokumenten gemacht wurden. Der Bericht wird in einer eigenen Datenbank (POLCYSYN.NSF) gespeichert.

Beim Starten des Reports kann angegeben werden, wie detailliert die Ausgabe sein soll:

- **detailliert**
  Alle Informationen (auch die Einstellungen) werden ausgegeben.
- **summiert**
  Nur die Richtlinien werden ausgegeben. Dabei wird die Struktur aller gültigen Richtlinien – also der hierarchischen und der speziellen – gedruckt.

Um die Richtlinienzusammenfassung aufzurufen, wird im Administrator-Client der Bereich „Personen“ ausgewählt, als Nächstes die Ansicht „Personen“. In der Werkzeugleiste am rechten Rand steht nun die Auswahl „Richtlinie“ zur Verfügung. In der folgenden Auswahlbox wird gewählt, ob der Bericht ausführlich oder detailliert erstellt werden soll. Ebenso kann die Berichtsdatenbank überschrieben werden, oder es wird ein Dokument in die bestehende Datenbank geschrieben. Je nach Wunsch kann die Datenbank lokal oder auf einem Server gespeichert werden. Falls die Datenbank erweitert wird, ist es auch später möglich, Einstellungen, die zu einem bestimmten Zeitpunkt galten, nachzuvollziehen.

Diese Seite ist zur Zeit nicht belegt.

9.7 Virenschutz unter Lotus Domino

Die Bedrohung durch Viren nimmt stetig zu. Die genaue Zahl der „Viren", „Trojanischen Pferde" und „Würmer" zu ermitteln, ist fast unmöglich, da pro Tag zwischen 15 und 20 neue Viren entdeckt werden (Anfang 1999 waren ungefähr 16.000 Viren bekannt, laut McAffee – Stand 04/2002 – sind es heute über 57.000). Dabei macht sich vor allem die zunehmende Verwendung von e-Mails und Internet bemerkbar. Die Verbreitung eines Virus bleibt nicht mehr regional, sondern erfolgt innerhalb weniger Stunden über die ganze Welt. Lotus Notes als e-Mail-System ist durch die integrierten Sicherheitsmechanismen von dieser Entwicklung zwar nicht völlig verschont, aber doch erheblich weniger betroffen. Um die Gefährdung weiter zu verringern, wird in vielen Firmen auf den Lotus Domino-Servern Antivirensoftware eingesetzt. Dadurch soll erreicht werden, dass Viren schon vor der Zustellung an den Adressaten unschädlich gemacht werden. Der Funktionsumfang einer Virensoftware gliedert sich dabei in mehrere Bereiche:

- **Kontinuierliche Echtzeit-Überwachung**
  von ein- und ausgehenden e-Mails während der Laufzeit des Servers

- **Zeitgesteuerte Überprüfung**
  von Mail-Datenbanken auf dem Server

- **Erstellung von Berichten**
  über die durchgeführten Maßnahmen und gegebenenfalls gefundenen Viren

- **Automatische und manuelle Aktualisierung**
  der Software und der Virenerkennungsdaten

Anhand der Antivirensoftware „GroupShield“ von McAffee soll im Folgenden gezeigt werden, wie eine solche Software installiert, eingerichtet und gewartet wird.

9.7.1 Installation

Von McAffee werden verschiedene Installationsmedien zur Auswahl angeboten. Es ist möglich die Software auf CD oder aus dem Internet über Download zu beziehen. (Eine Testversion kann von www.mcaffee.com heruntergeladen werden, um die folgenden Schritte nachzuvollziehen.) Da täglich Änderungen an der Software und den Virendefinitionen erfolgen, ist es wichtig, auf jeden Fall die aktuellen Upgrades aus dem Internet zu laden und nach der Installation der eigentlichen Software ebenfalls einzuspielen. Da sich die für die Installation notwendigen Voraussetzungen ständig ändern, müssen sie vor der Installation anhand der aktuellen Dokumentation geprüft werden.

GroupShield für Domino kann nicht eingesetzt werden, wenn unterschiedliche Versionsstände von Lotus Domino auf dem selben Rechner installiert sind.

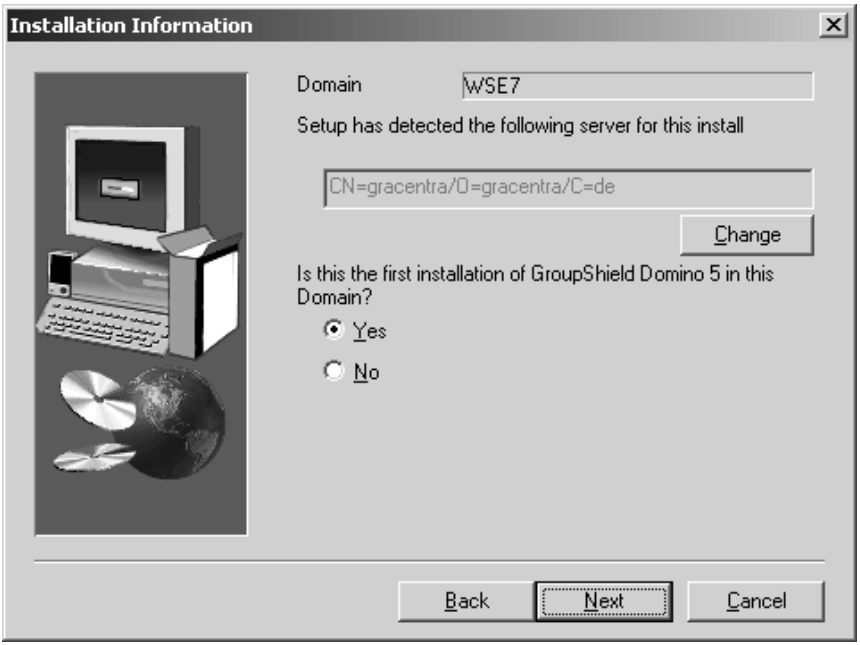
Zunächst erfolgt die Anmeldung am NT-Server, auf dem der Lotus-Domino-Server läuft, mit einem Benutzer, der Administratorrechte besitzt. Bei dem Entpacken der Software wird ein temporäres Verzeichnis angelegt und die Software entweder von der CD in dieses Verzeichnis kopiert oder aus einem Archiv aus dem Internet in das Verzeichnis entpackt. In dem temporären Verzeichnis steht nun ein SETUP-Programm, das durch Doppelklicken gestartet werden kann. Auch das sollte erst nach dem Lesen der beigefügten „Readme"-Datei erfolgen.

9.7.1.1 Installationsverlauf

Zunächst wird nach dem Start ein Installationsfenster geöffnet. Es weist darauf hin, dass alle laufenden Programme beendet werden sollen, bevor mit der Installation fortgefahren werden kann. Dabei sind insbesondere **ALLE** Lotus-Domino-Server und alle Lotus-Notes-Clients auf dem Server zu beenden.

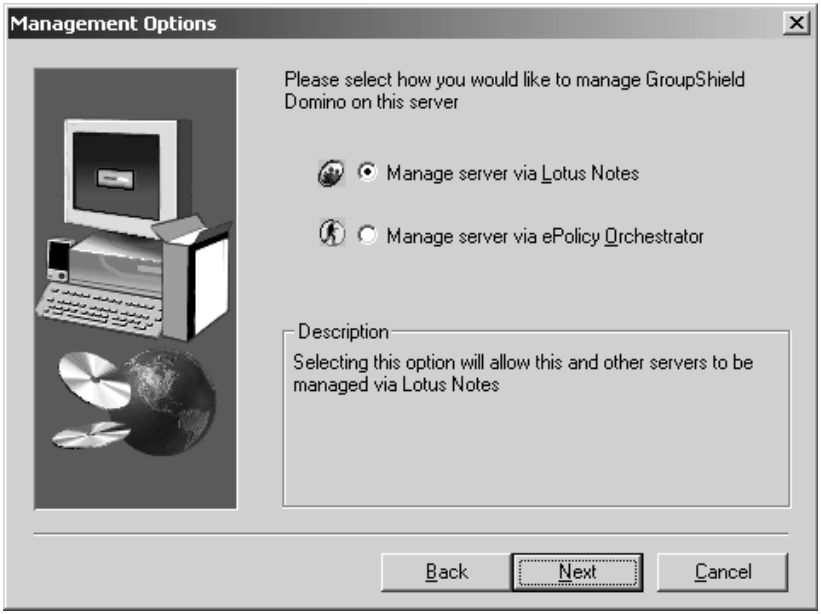
Start der Installation

Als Nächstes wird der Server abgefragt, für den die Installation durchgeführt werden soll, ob es sich um das erste Mal handelt, dass GroupShield in dieser Domäne eingespielt wird.



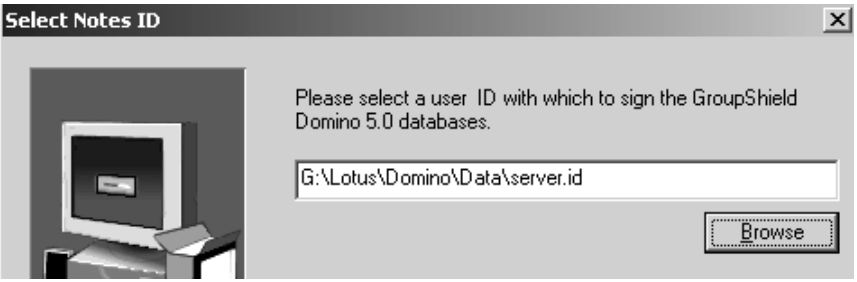
Auswahl des Servers

Die aktuelle Version der GroupShield-Antivirensoftware bietet die Möglichkeit, über Lotus Notes oder über einen „ePolicy Orchestrator“ – einem Hilfsprogramm aus GroupShield – verwaltet zu werden. In diesem Beispiel wird auf externe Werkzeuge verzichtet und mit dem Lotus-Notes-Client gearbeitet.



Administrations-Client festlegen

Um auf Lotus-Domino-Datenbanken zugreifen zu können, muss eine ID-Datei bereitgestellt werden, deren Benutzer die notwendige Administrator-Berechtigung hat.



ID festlegen

In unserem Beispiel wurde die Server-ID verwendet. Im folgenden Dialog wird der Pfad eingestellt, unter dem installiert werden soll. Bei der Frage nach dem Typ ist die Auswahl „Standardinstallation“ ausreichend, es sei denn man möchte auf die Installation der Dokumentation verzichten.

Setup-Typ auswählen

In den restlichen Dialogen werden die üblichen Auswahlen zu Menüpunkten usw. abgefragt, die aus der Standardeinstellung übernommen werden können.

9.7.1.2 Welche Datenbanken werden installiert?

Zur Durchführung der verschiedenen Aufgaben bei der Virenüberwachung werden eine ganze Reihe von Datenbanken erstellt:

- **Konfiguration**
  Die Konfiguration erfolgt in einer Datenbank mit dem Namen „GSDConfig.nsf". Die Steuerung aller Dominoserver einer Domäne, die von GroupShield überwacht werden sollen, erfolgt über diese Datenbank.

- **Protokolle**
  Die Speicherung der Protokolle, die während der Laufzeit erstellt werden, erfolgt in der Datenbank „GSDLog.nsf". Hier werden vor allem die durchgeführten Aktionen und Maßnahmen gespeichert, die ergriffen wurden, wenn verdächtige Inhalte gefunden wurden.

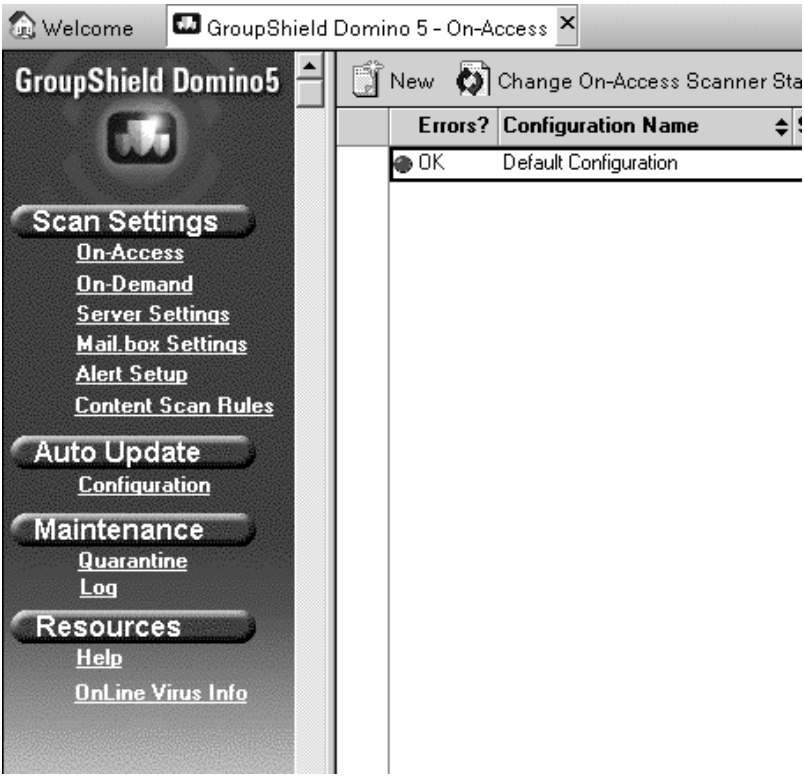
- **Quarantäne**
  Wenn GroupShield für Domino verdächtige Lotus-Notes-Dokumente oder Datei-Anhänge entdeckt, werden sie getrennt in der Datenbank mit dem Namen „GSDQuarantine.nsf" gespeichert. In dieser Quarantäne-Datenbank können Elemente angezeigt und verwaltet werden, die gesperrt wurden.

- **Update**
  Alle neuen Versionen der GroupShield-Scanmodule und der Virus-Definitionsdateien für den Groupshield-Domino-Scanner werden in der Update-Datenbank gespeichert.

- **Hilfe**
  Die aktuelle Hilfe zu GroupShield Domino befindet sich in der Datenbank GSDHelp.nsf.

9.7.1.3 Administration und Einrichtung

Die Administration erfolgt bei der vorgenommenen Einstellung über den Lotus-Notes-Client. Bei der Installation wird ein Menüeintrag erstellt, der die entsprechende Datenbank startet. Von diesem Punkt aus werden alle Einstellungen und Kontrollen durchgeführt: die Einstellung der verschiedenen Parameter, das Starten des automatischen Updates, die Kontrolle und Wartung der durchgeführten Aktionen und der Zugriff auf die Hilfedateien.



Funktionsübersicht

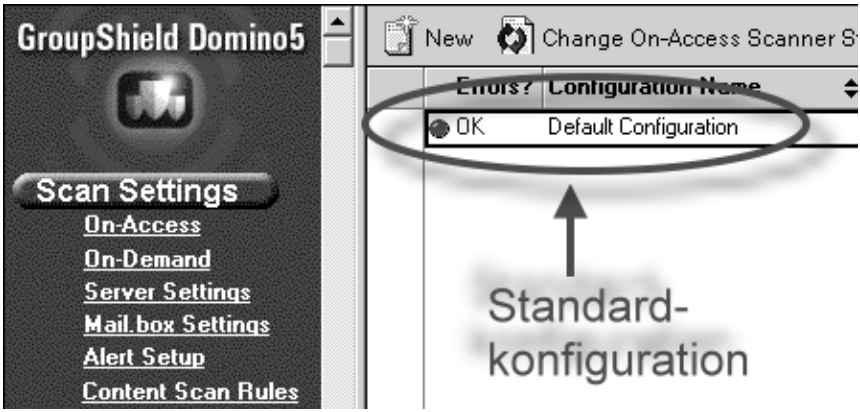
9.7.2 Einstellungen

Beim Scannen nach Viren muss aus Performance-Gründen in der Regel ein Kompromiss gefunden werden: zwischen dem kompletten Scannen aller e-Mails und damit „vollständiger Sicherheit“ auf der einen Seite und der dafür notwendigen Rechnerkapazität auf der anderen Seite. Es wird unterschieden in „Kontrolle im laufenden Betrieb“ und „Kontrolle zu den Zeitpunkten, zu denen der Server nicht oder nur sehr wenig frequentiert wird“.

Die anderen Einstellungen regeln, wie sich die Software auf dem Server verhält und was geschehen soll, wenn ein Virus in einer e-Mail enthalten ist.

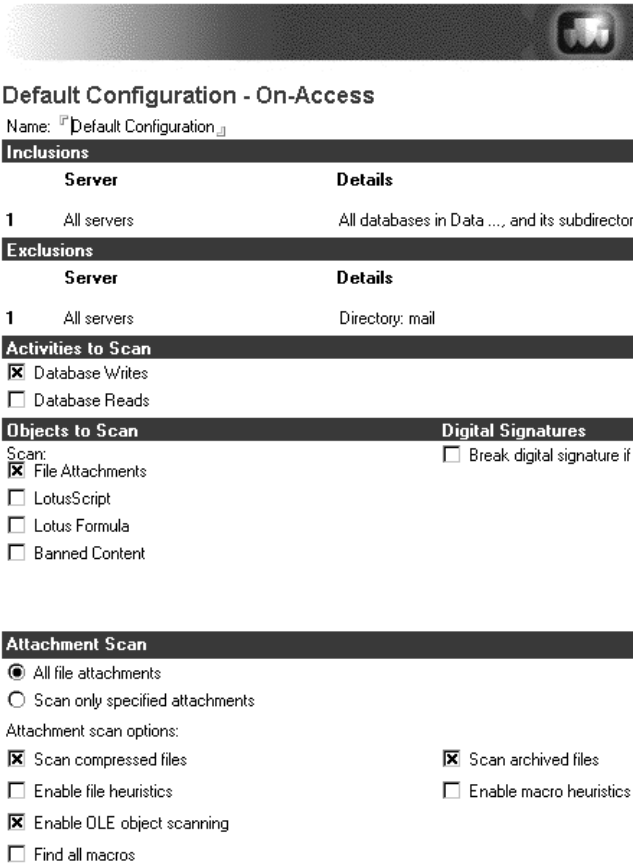
9.7.2.1 Zugriff im laufenden Betrieb

Beim Start der GroupShield-Datenbank ist der erste Menüpunkt schon ausgewählt und die Standardkonfiguration wird angezeigt.



Standardkonfiguration

Durch Doppelklicken kann die bestehende Konfiguration für die Bearbeitung geöffnet werden. Über die Schaltfläche „Neu in der Aktionsleiste“ kann eine weitere Konfiguration hinzugefügt werden. Dies ist z. B. der Fall, wenn für einen bestimmten Server andere Einstellungen gelten sollen, als im Standard vorgegeben. Die mitgelieferte Standardkonfiguration ist so angelegt, dass sie für alle Server gilt, für die keine besondere Festlegung getroffen wurde.



Einstellungen der Standardkonfiguration

Unter der Überschrift „Inclusions“ können ein, mehrere oder alle Server für die Überwachung ausgewählt werden. Je Server kann definiert werden, für welche Verzeichnisse die Einstellungen gelten und ob Unterverzeichnisse ebenfalls mit gescannt werden sollen. Unter der Überschrift „Exclusions“ werden Server aufgeführt, die nicht mit eingeschlossen werden sollen. Beim nächsten Punkt geht es um Performance.

Unter „Activities to Scan“ kann angeklickt werden, ob beim Schreiben und beim Lesen gescannt werden soll. Hier ist Vorsicht geboten, da dies erhebliche Auswirkung auf die Performance des oder der Domino-Server haben kann. Normalerweise kann kein Virus in eine Datenbank kommen, wenn vor dem Schreiben geprüft wird, ob die e-Mail einen Virus enthält. Lediglich, wenn in bestehenden Datenbanken schon Viren sind, könnte dieser Fall eintreten. Dann würde aber die Verbreitung verhindert werden, weil der Virus beim Schreiben (das überwacht wird) gefunden würde. Hinzu kommt, dass normalerweise eine regelmäßige Prüfung aller Datenbanken z. B. am Wochenende durchgeführt wird.

Im Abschnitt „Objects to Scan“ wird eingestellt, welche Anhänge und Daten gescannt werden sollen.

Auch hier gilt, dass die Performance des Servers leidet, je mehr Objekte geprüft werden sollen.

Wenn auch verschlüsselte und signierte e-Mails geprüft werden sollen, muss der Punkt „Break Digital Signature if Necessary“ angeklickt werden. Innerhalb der Dateianhänge kann noch feiner unterteilt werden, welche Anhänge gescannt werden sollen und wie dies geschehen soll.

Um auch auszuschließen, dass ein Server oder ein Benutzer dadurch attackiert wird, dass sehr große oder sehr viele Anhänge an eine Datei gehängt werden, kann unter „Attachment Blocking“ der Punkt „Block Attachements by Size“ und „Block Attachements by Number“ angeklickt werden.

Im letzten Abschnitt wird eingestellt, was passieren soll, wenn ein Virus gefunden wurde.

9.7.2.2 Zeitgesteuerte Kontrolle

Hinter dem Punkt „On-Demand“ verbirgt sich der zeitgesteuerte Aufruf des Antiviren-Scanners. Dies wird vor allem verwendet, um regelmäßig – z. B. am Wochenende – alle Datenbanken zu überprüfen. Ähnlich wie bei den Einstellungen für die Prüfung während des laufenden Betriebs wird hier zunächst angegeben, für welche Server diese Konfiguration gelten soll und für welche nicht. Unter dem Abschnitt „Schedule“ erfolgt dann die Auswahl der Tage und Uhrzeiten, zu denen gescannt wird. In einem weiteren Abschnitt wird eingestellt, welche Dokumente (Daten oder Design) mit gescannt werden sollen und welche Priorität der Scan-Task haben soll. Außerdem kann auch inkrementell gescannt werden, damit nicht immer wieder alle Dokumente gescannt werden müssen. Auch hier kann – wie oben beschrieben – die Art der zu scannenden Objekte und Anhänge eingegrenzt werden.

On-Demand Monitor

Name: Custom Configuration 1

Inclusions

Server	Details

Exclusions

Server	Details

Schedule ◉ Enabled ○ Disabled

Schedule options:

- ○ On startup
- ○ Run once only
- ◉ Schedule by week
- ○ Schedule by month

Time(s) to run: 22:47 (you can enter multiple time ranges - i.e. 15:00; 22:00 -

Repeat every: 60 Minutes (only used where you have

Day(s) of week to run on:

☒ Mon ☐ Tue ☐ W
☐ Fri ☐ Sat ☐ Su

Type of Scan

- ◉ Data Documents
- ○ Design Documents

Incremental Scanning

- ◉ Off
- ○ On - from date specifie
- ○ On - from last scanned

CPU Utilization:
low <- ○ 1 ○ 2 ◉ 3 ○ 4 ○ 5-> high

Objects to Scan

Scan:
☒ File Attachments

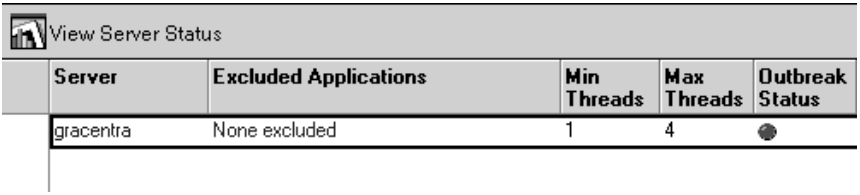
Digital Signatures

☐ Break digital signature

Einstellungen des zeitgesteuerten Zugriffs

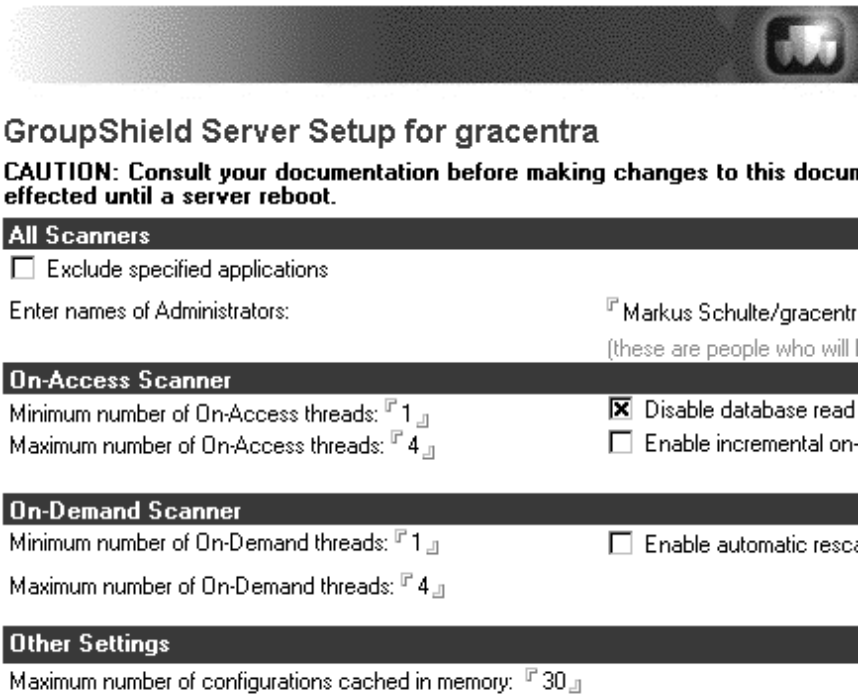
9.7.2.3 Server-Einstellungen

Für jeden Server können Einstellungen zu den Aufgaben, die zum GroupShield-Antivirenscanner gehören, und deren Status vorgenommen werden.



Server verwalten

Mit Doppelklicken wird ein Server für die Bearbeitung geöffnet.

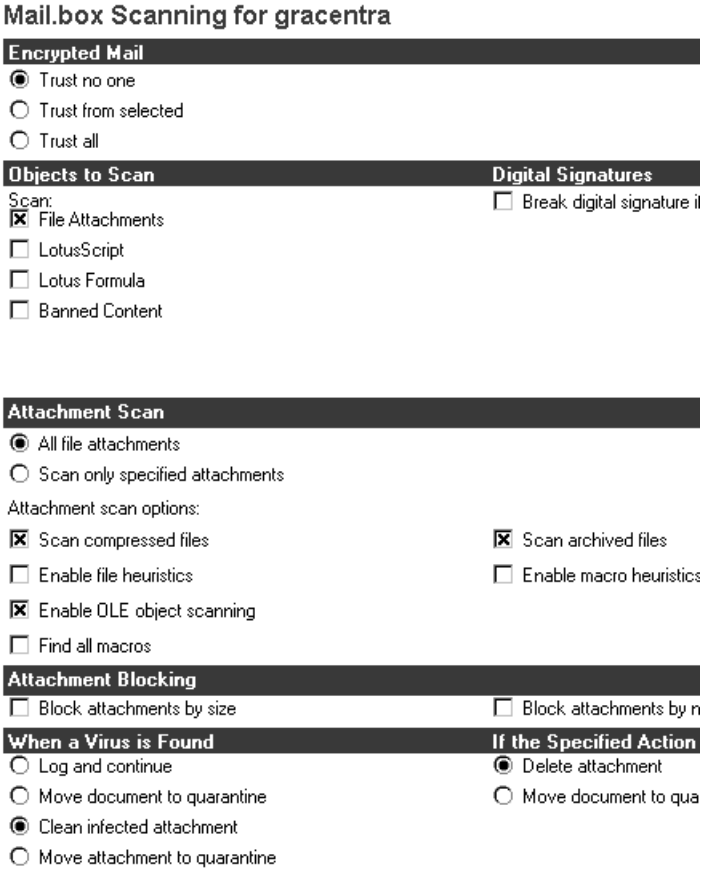


Server-Einstellungen festlegen

Unter der ersten Rubrik „All Scanners“ wird festgelegt, ob bestimmte Anwendungen vom Scannen ausgeschlossen werden sollen und wer für die Administration der Scan-Task auf dem Server verantwortlich ist. Danach können die Ressourcen für die verschiedenen Scan-Prozesse eingestellt werden. In der Regel kann hier die Standardkonfiguration beibehalten werden.

9.7.2.4 Einstellungen für die Datenbank „Mail.box“

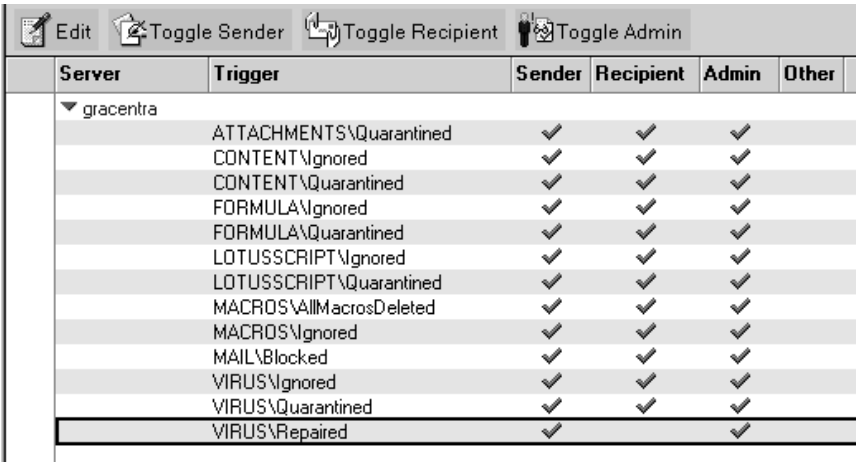
Für die Mailrouting-Datenbank „Mail.box“ des ausgewählten Servers kann unter dem Punkt „Verschlüsselte e-Mail“ eingestellt werden, von wem verschlüsselt e-Mails als vertrauenswürdig eingestuft werden sollen. Dann folgen die schon bekannten Einstellungen zu den Objekten und Dateianhängen, die gescannt werden sollen.



Einstellungen zur Mail-Box festlegen

9.7.2.5 Einstellungen Alarmierung

Ist ein Virenbefall festgestellt worden, sollten ein Administrator und die betroffenen Personen benachrichtigt werden. In den Alarm-Einstellungen wird eingestellt, welche Personen bei den verschiedenen Ereignissen, die einen Alarm auslösen, informiert werden sollen.



Server	Trigger	Sender	Recipient	Admin	Other
gracentra					
	ATTACHMENTS\Quarantined	✓	✓	✓	
	CONTENT\Ignored	✓	✓	✓	
	CONTENT\Quarantined	✓	✓	✓	
	FORMULA\Ignored	✓	✓	✓	
	FORMULA\Quarantined	✓	✓	✓	
	LOTUSSCRIPT\Ignored	✓	✓	✓	
	LOTUSSCRIPT\Quarantined	✓	✓	✓	
	MACROS\AllMacrosDeleted	✓	✓	✓	
	MACROS\Ignored	✓	✓	✓	
	MAIL\Blocked	✓	✓	✓	
	VIRUS\Ignored	✓	✓	✓	
	VIRUS\Quarantined	✓	✓	✓	
	VIRUS\Repaired	✓		✓	

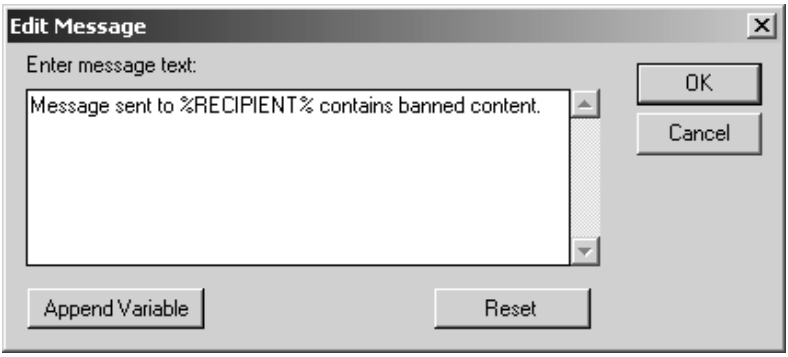
Einstellungen zur Alarmierung festlegen

9.7.2.6 Einstellung Benachrichtigung

Wenn eine E-Mail einen Virus enthält, muss festgelegt werden können, wer benachrichtigt werden soll und auf welche Weise. Die Einstellungen dafür werden in der Maske „E-Mail Alarm Nachricht für <Name des Servers>“ vorgenommen. Es kann eine E-Mail an folgende Adressaten gesendet werden, wenn ein Virus gefunden wurde:

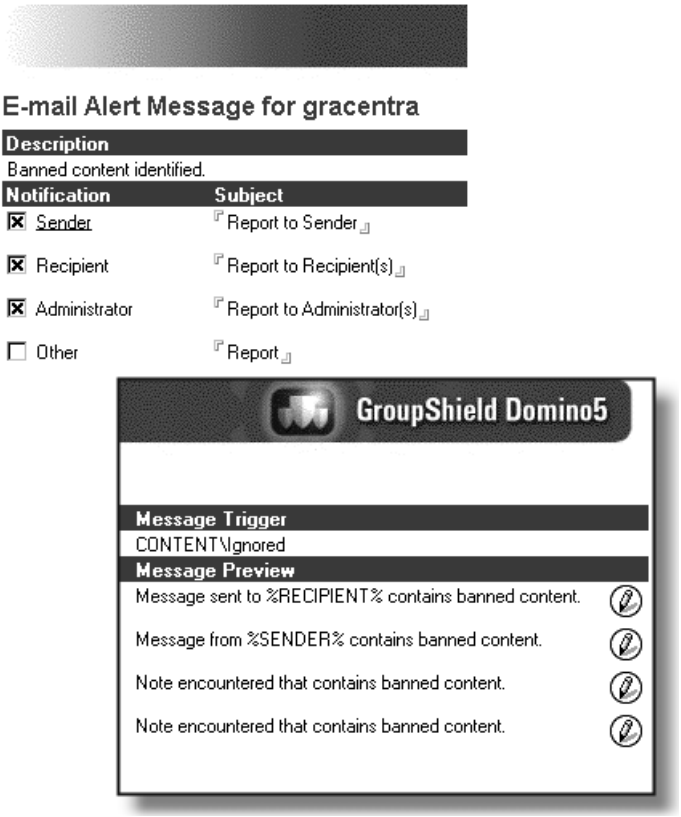
- an den Absender der E-Mail,
- an den Empfänger der E-Mail,
- an den Administrator (wobei hier der Administrator für Groupshield gemeint ist)
- und an einen beliebigen zusätzlichen Empfänger.

Für jeden dieser Adressaten kann als Erstes das Betreff-Feld angegeben werden, mit dem die E-Mail abgeschickt wird. Als Nächstes wird der eigentliche Text, der in der E-Mail stehen soll, festgelegt. Um Informationen über Absender und Empfänger der E-Mail gleich bei der Warnung mit angeben zu können, gibt es zwei Variablen: %RECIPIENT% und %Sender%.



V*ariable für den Benachrichtigungstext*

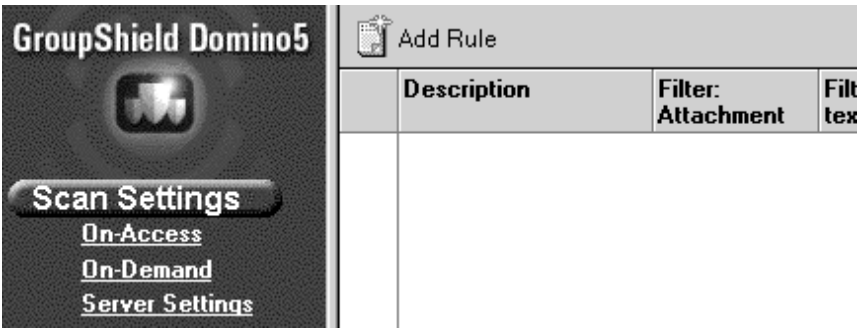
Wenn diese Variablen in dem Text vorkommen, werden sie vor dem Versenden der Benachrichtigung durch den Absender bzw. den Empfänger der E-Mail ersetzt. Am Ende jeder Zeile ist eine Schaltfläche zu sehen, über die ein Abfragefeld für die E-Mail-Adresse des Empfängers geöffnet wird.



Einstellungen zu den Benachrichtigungen

9.7.2.7 Einstellung zusätzlicher Regeln

Diese Funktion erlaubt es dem Administrator, zusätzliche Regeln zu erstellen, um unerwünschte E-Mails und E-Mail-Anhänge auszusondern. Hier kann zum Beispiel eine Regel zum Aussortieren von Spam-Mails erstellt werden. Ebenso können E-Mails, deren Subjekt-Feld einem bestimmten Begriff entsprechen, ausgefiltert werden.



Regeln hinzufügen

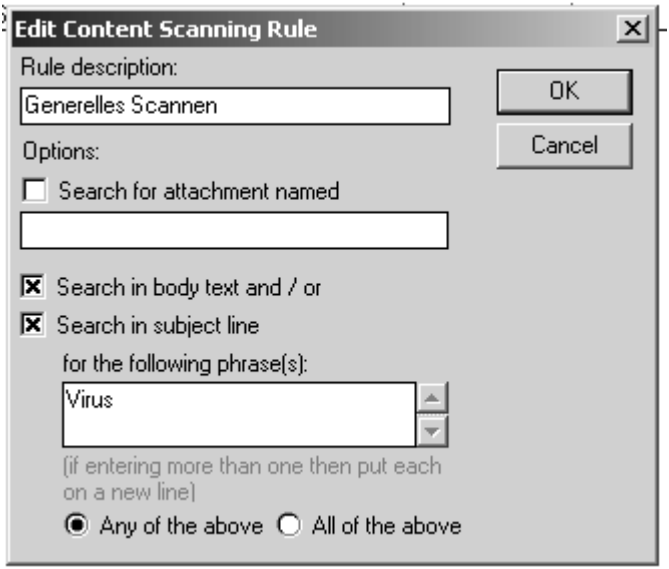
In der Ansicht „Scan-Regeln für Inhalte“ kann durch Klicken auf die Schaltfläche „Regel hinzufügen“ eine neue Regel erstellt werden. Die Dokumente mit bereits vorhandenen Regeln können geöffnet und bearbeitet werden. In der Ansicht sind folgende Informationen aufgeführt:

- der Name der Regel,
- die Regeln für E-Mail-Anhänge,
- die Regeln für den eigentlichen E-Mail Text und
- die Regeln für Betreff/Subjekt der E-Mail.

In der Maske zum Bearbeiten der Regel wird zunächst der Name der Regel festgelegt. Für die Definition der Filterkriterien kann zwischen mehreren Möglichkeiten gewählt werden:

- Suche nach einem Anhang mit einem bestimmten Namen und/ oder
- Suche im eigentlichen Text der E-Mail und/oder
- Suche im Betreff der E-Mail.

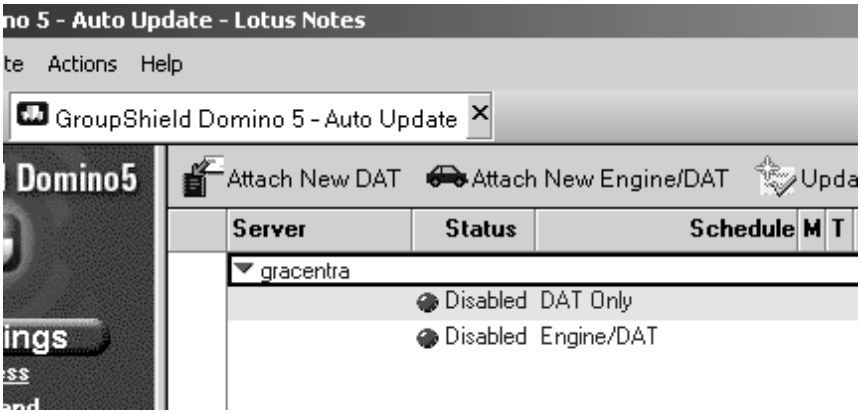
Im nächsten Feld können ein Wort oder mehrere Suchbegriffe eingegeben werden. Zusätzlich kann man auswählen, ob die E-Mail alle Begriffe enthalten muss, damit der Filter gilt oder ob bereits einer der Begriffe ausreichend ist.



Regel bearbeiten

9.7.2.8 Einstellung/Aktualisierung

Um Viren erkennen zu können, werden bestimmte Muster von Byte-Folgen innerhalb der Daten gesucht und in eine Datei gespeichert. Wenn eine Datei diese Byte-Folge enthält, ist die Wahrscheinlichkeit, dass es sich um eine infizierte Datei handelt, sehr hoch. Wenn neue Viren auftauchen, wird zu diesen eine entsprechende Folge ermittelt. Damit der Virenscanner diese neuen Viren erkennen kann, benötigt er eine möglichst aktuelle Version dieser Datei. Diese wird von McAffee (und den Herstellern anderer Antiviren-Software) ständig aktualisiert und im Internet zur Verfügung gestellt. Natürlich kann es auch sein, dass die Software, mit der die Dateien durchsucht werden, um zusätzliche Möglichkeiten ergänzt werden muss. Für beide Fälle besteht die Möglichkeit unter dem Punkt „Auto Update“ Dateien, die aus dem Internet geladen wurden, einzuspielen. Dieser Vorgang kann auch automatisch erfolgen. Hierbei ist allerdings Vorsicht geboten. Da die Umgebungen, in denen die Software und die DAT-Dateien eingesetzt werden, sehr unterschiedlich sind, kann es zu Inkompatibilitäten kommen. Wird ein solches Update automatisch eingespielt, kann es sein, dass überhaupt kein Scannen und damit auch kein Schutz gegen Viren mehr möglich ist.



Auto Update

Wenn die Aktualisierung gewünscht ist, kann durch Doppelklicken auf den entsprechenden Punkt die Bearbeitungsmaske aufgerufen werden. Die Maske erfragt zunächst, ob die Aktualisierung zeitgesteuert und automatisch erfolgen soll. Dann wird ausgewählt, für welche Plattformen (Windows NT oder UNIX) die DAT-Daten bzw. Programme übertragen werden sollen. Falls die Dateien regelmäßig aus dem Internet geladen werden, können sie über die Option "Von einem lokalen Server kopieren" eingespielt werden. Sie können aber auch aus einer entsprechenden Datenbank direkt aus dem Internet geladen oder über FTP geholt werden. Danach wird der Zielpfad für die Datei einstellt. Wenn nach dem Update ein Programm gestartet werden soll, ist die entsprechende Option anzuhaken.

9.7.3 Wartung/Kontrolle

Für Kontrolle der durchgeführten Aktionen von Groupshield gibt es zwei Ansichten, in denen Protokolldokumente und verdächtige E-Mails aufgelistet sind:

- Groupshield-Protokolle und
- Groupshield-Quarantäne

9.7.3.1 Groupshield-Protokolle

Unter der Ansicht „Protokolle“ finden sich Dokumente mit allen Ereignissen, die Groupshield betreffen. Hierzu gehören:

- das Einspielen der aktualisierten Virendefinitionsdateien und
- die Durchführung automatischer Kontrollen auf Viren

Der Übersicht halber können entweder alle, nur die heutigen oder alle Ereignisse der letzten 7 Tage angezeigt werden.

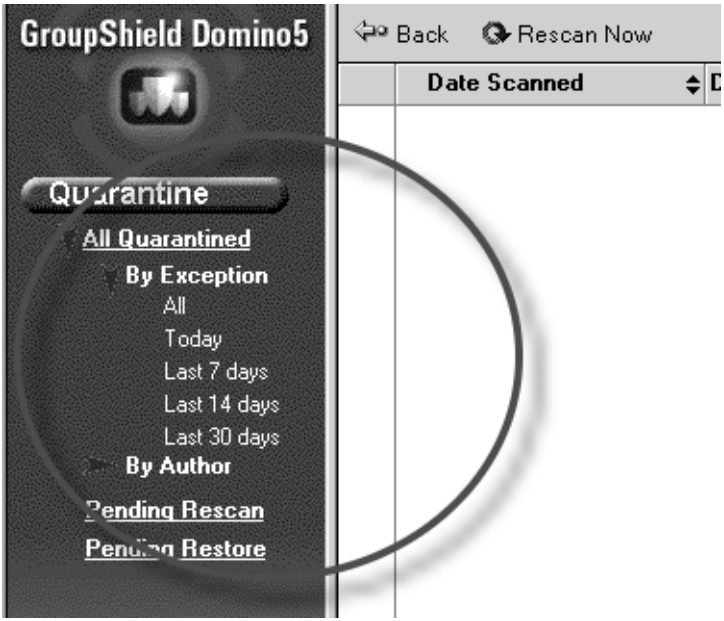
Protokoll-Ansichten

Zusätzlich bietet Groupshield Ansichten, in denen Dokumente angezeigt werden, die

- nur die Ereignisse „Manuelle Scan-Aufrufe“ enthalten,
- durch „Automatischer Update“ ausgelöst wurden oder
- „Per Virus“ sortiert sind.

9.7.3.2 Groupshield-Quarantäne

In der Ansicht Quarantäne können alle e-Mails, die in Quarantäne geschoben wurden, kontrolliert werden. Dabei kann – wie auch bei den Protokollen – zunächst nach Zeit (d.h.: wie lange das Ereignis her ist) unterschieden werden und anschließend nach dem Ersteller der E-Mails.



Quarantäne-Ansichten

In der Ansicht ist erkennbar, wann der Scan-Lauf stattgefunden hat, in welcher Datenbank der Virus gefunden wurde sowie welche Versionsstände die Scan-Software und die Virensignaturdatei zu dem Zeitpunkt hatte, als der Virus in Quarantäne geschoben wurde.

9.8 Serverbasierte Spam-Abwehr

So unverzichtbar der Austausch von elektronischer Post für den Erfolg der meisten Unternehmen geworden ist, so lästig ist die ständig steigende Anzahl von unerwünschten Poststücken in den Poseingangskörben der Mitarbeiter. Untersuchungen haben gezeigt, dass 10-50 Prozent aller eingehenden Nachrichten vom Empfänger weder angefordert noch erwünscht sind. Ganz abgesehen von der Tatsache, dass die ständig steigende Zahl der zu bewältigenden e-Mails zu einem erheblichen Stressfaktor für die Mitarbeiter werden kann, ist der Aufwand zum Sichten und Löschen solcher Junk-Mails oder Spams zeit- und kostenintensiv. Noch problematischer ist die Gefahr, dass in dieser Flut wirklich wichtige Nachrichten untergehen und vom Benutzer übersehen bzw. versehentlich gelöscht werden.

Versender von Spam sammeln u. a. die e-Mail-Adressen ihrer Opfer aus öffentlich zugänglichen Quellen – wie z.B. Anwenderforen oder Mail-Listen – oder sie erwerben diese von unseriösen Unternehmen, die die e-Mail-Adressen Ihrer Kunden weiterverkaufen. Von daher gibt es grundsätzlich Möglichkeiten, das Einsammeln der eigenen e-Mail-Adresse zu vermeiden bzw. zu erschweren. Denkbar ist z.B. bei einem kostenlosen Mail-Service – wie web.de oder gmx – ein Mail-Konto anzulegen und die entsprechende e-Mail-Adresse bei der Registrierung auf Web-Seiten oder Foren zu verwenden. Auch wenn eine solche Vorgehensweise das Spam-Volumen deutlich reduzieren kann, lässt sie sich im betrieblichen Umfeld schwer oder überhaupt nicht durchsetzen.

Bis „wasserdichte“ Verfahren zur Verhinderung von Spam entwickelt worden sind, kann das Problem nur mit mehr oder weniger

erfolgreichen Mitteln reduziert werden. Es wird Junk-Mails geben, die trotz aller Bemühungen den Posteingangskorb eines Anwenders erreichen und ebenso wird die eine oder andere unbedenkliche e-Mail zu Unrecht als Spam angesehen. Die Herausforderung ist, eine besonders hohe Trefferquote bei einer geringen Anzahl von Fehlalarmen zu erreichen und das ganze noch mit geringem Administrationsaufwand.

Im Folgenden werden einige Möglichkeiten vorgestellt und bewertet, die Spam-Flut einzudämmen. Hierbei werden Bordmittel von Domino beschrieben und einige ausgewählte Zusatzprodukte vorgestellt.

Bordmittel:

- Reverse Lookup
- Absender-Domäne im DNS verifizieren
- DNS Blacklists
- Verhinderung von SMTP-Mail an Gruppen
- Mail nur für Adressen im Adressbuch annehmen
- Server Mail-Regeln

Zusatzprodukte:

- Scanmail Suite (eManager)
- Open Source-Projekt SpamAssassin
  - in Appliances wie z.B. Tuxgate oder BenHur
  - als Windows-Software No-Spam-Today

9.8.1 Bordmittel von Domino

Reverse Lookup

Versender von Spam – so genannte Spammer – versuchen mit verschiedenen Verfahren, ihre Identität bzw. die Herkunft der e-Mails zu vertuschen. Spammer verwenden so genannte „Offene Relays“, versenden Ihre e-Mails über Computer, die sich über eine dynamische IP-Adresse mit dem Internet verbinden oder nutzen sogar beliebige Rechner, die über einen per Virus eingepflanzten Trojaner Spam weiterleiten.

Reverse Lookup versucht die e-Mail, die über solche Wege verteilt wird, zu erkennen und zu blockieren. Verbindet sich ein sendender Computer mit Domino, wird in der Startphase der Kommunikation der Absender-Hostname übermittelt. Der Domino-Server nimmt diesen Hostnamen und die IP-Adresse des sendenden Rechners und verifiziert im DNS, ob diese zusammenpassen. Hierzu wird der so genannte PTR (Pointer) Record abgefragt.

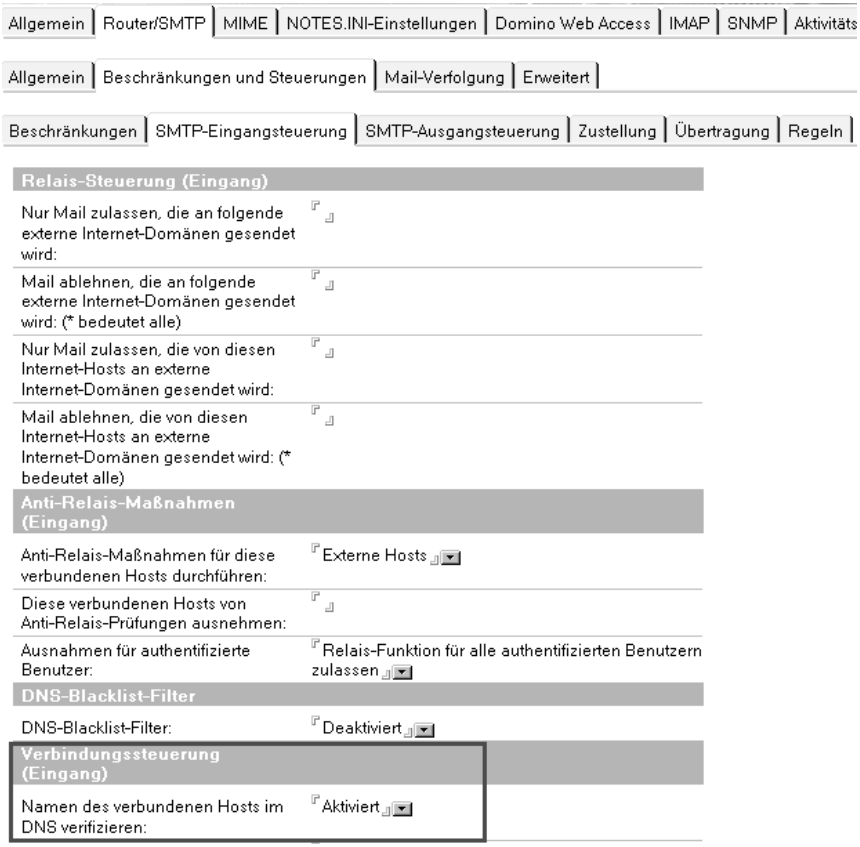
Da Spammer unerkannt bleiben möchten, kann man davon ausgehen, dass solch ein passender PTR Record nicht gefunden werden kann. Falls doch, könnte die Identität bzw. die Herkunft eines Spammers leicht ermittelt werden.

Nachteil dieser Lösung ist, dass ein PTR Record bei der Anlage einer Mail-Domäne nicht automatisch angelegt wird und von daher auch viele „saubere“ Mail-Server im Internet nicht über einen solchen PTR Record geprüft werden können. Die Folge ist, dass auch eine unbedenkliche e-Mail vom Domino abgewiesen wird.

Tipp:

Egal, ob Sie Reverse Lookup einschalten oder nicht, fragen Sie Ihren ISP, ob für Ihren eigenen Mail-Server ein PTR Record angelegt ist. Falls nicht, lassen Sie einen solchen anlegen. Es könnte sein, dass ein Geschäftspartner gerade den Reverse Lookup aktiviert und sie keine e-Mail mehr an ihn senden können.

Der Reverse Lookup wird im Domino-Verzeichnis (Datei „names.nsf“ auf dem Domino-Server) im Server-Konfigurationsdokument (vgl. Teil 2 Kapitel 4. 4. 1) aktiviert. Das Konfigurationsdokument finden Sie bei R5 in der Ansicht „Server“, „Konfigurationen“ und bei R6 in „Konfiguration“, „Nachrichtenaustausch“, „Konfigurationen“. Im Abschnitt „Router/Smtp“, „Beschränkungen und Steuerungen“, „SMTP-Eingangssteuerung“, „Verbindungssteuerung (Eingang)“ ist das Feld „Namen des verbundenen Hosts im DNS verifizieren“ auf „Aktiviert“ zu setzen.



Reverse Lookup

Absender-Domäne im DNS verifizieren

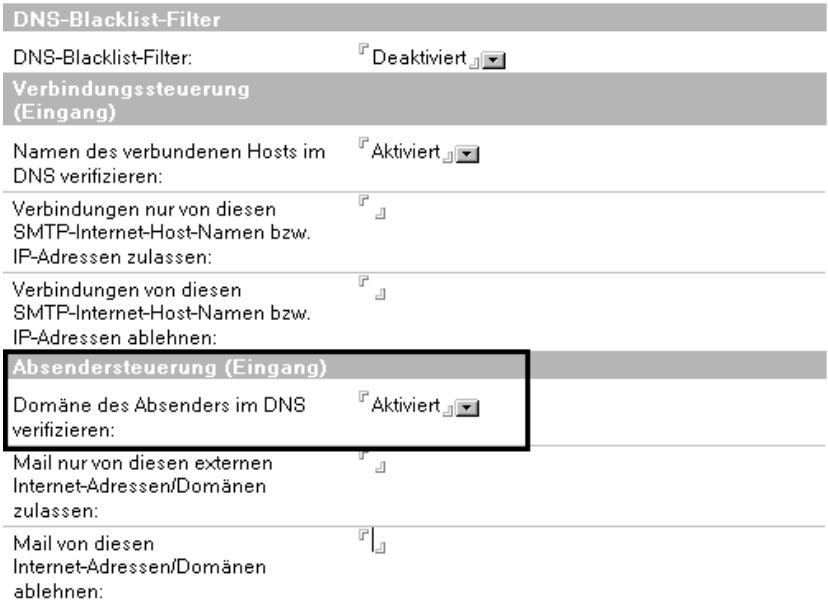
Vor der Annahme einer e-Mail wird geprüft, ob es die Domäne in der e-Mail-Adresse des Absenders im DNS überhaupt gibt. Da Spam und Viren in der Absender-Adresse manchmal nicht existierende Domänen-Namen angeben, kann anhand dieser Prüfung eine solche Mail erkannt werden.

Beispiel für eine solche erfunden Absenderadresse:

mike@abcde1234.de

Dieses Verfahren wird bereits häufig eingesetzt und erfüllt im Rahmen des Möglichen seinen Zweck. Das Risiko, erwünschte Mails abzuweisen, ist recht gering.

Die Funktion wird im Domino-Verzeichnis (Datei „names.nsf“ auf dem Domino-Server) im Server-Konfigurationsdokument (vgl. Teil 2 Kapitel 4. 4. 1) aktiviert. Das Konfigurationsdokument finden Sie bei R5 in der Ansicht „Server“, „Konfigurationen“ und bei R6 in „Konfiguration“, „Nachrichtenaustausch“, „Konfigurationen“. Im Abschnitt „Router/Smtp“, „Beschränkungen und Steuerungen“, „SMTP Eingangssteuerung“, „Verbindungssteuerung (Eingang)“ ist das Feld „Domäne des Absenders im DNS verifizieren:“ auf „Aktiviert“ zu setzen.



Absender-Adresse im DNS verifizieren

DNS Blacklists (ab R6)

Unter DNS Blacklists versteht man Verzeichnisse mit den IP-Adressen von Computern, über die bereits Spam versendet wurde oder die technisch geeignet sind, Spam zu versenden oder weiterzuleiten. Einige dieser Verzeichnisse lassen sich kostenlos abfragen, andere stellen Ihren Dienst nur gegen Gebühr zur Verfügung.

Auch wenn – gerade die kostenlosen – DNS Blacklists eine einfache und bereits häufig eingesetzte Methode zur Spam-Vermeidung sind, gibt es doch zwei unangenehme Nebeneffekte. Zum einen ist

die Fehlerquote sehr hoch, da nicht jede e-Mail, die von einem gelisteten Rechner kommt, auch wirklich eine Spam ist. Zum anderen muss der Administrator regelmäßig prüfen, ob der angefragte Blacklist-Server noch arbeitet. Gerade die kostenlosen Dienstleister stellen Ihren Service ohne Vorwarnung ein. Daneben ist es nicht einfach, den oder die „richtigen" Dienstleister auszuwählen. Fast jeder Blacklist-Server beschränkt sich auf eine bestimmte Kategorie von gelisteten Servern (z.B. nur offene Relays, nur dynamische IP-Adressen). Im Bedarfsfall kann durch die Eingabe des Suchbegriffes „DNS Blacklist" in den Internet-Suchmaschinen eine umfangreiche Liste der Anbieter abgerufen werden. Welche IP-Adressen der jeweilige Anbieter unter welchen Bedingungen aufführt und welche IP-Adresse zur Abfrage in der Konfiguration des SMTP-Servers eingetragen werden muss, wird auf den jeweiligen Informationsseiten der Anbieter erläutert.

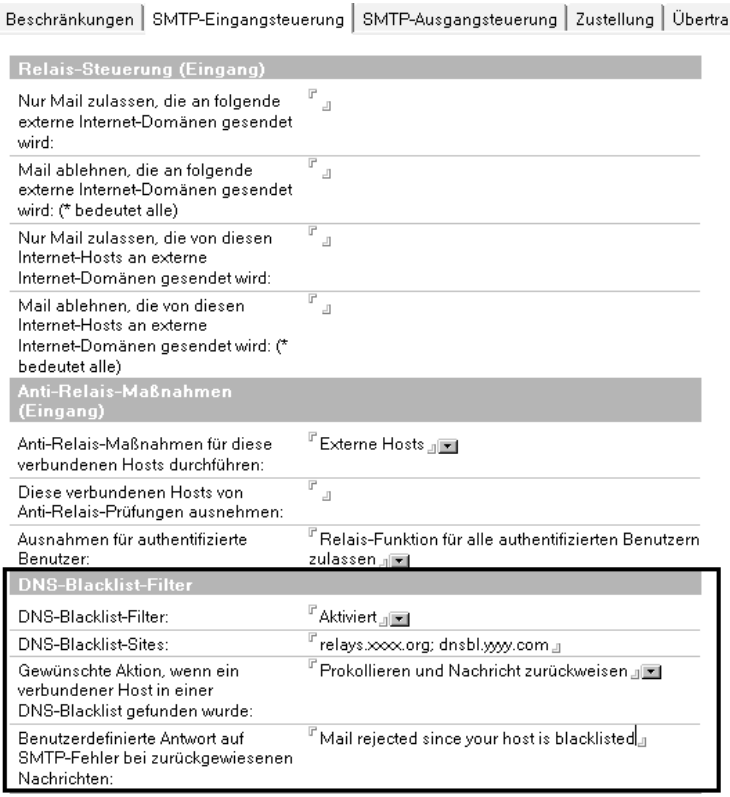
Um den Domino-Server beim Empfang einer e-Mail eine oder mehrere solcher Blacklists abfragen zu lassen, müssen im Domino-Verzeichnis (Datei „names.nsf" auf dem Domino-Server) die entsprechenden Hostnamen im Server-Konfigurationsdokument (vgl. Kapitel 4. 4. 1) eingetragen werden. Das Konfigurationsdokument finden Sie in der Ansicht „Konfiguration", „Nachrichtenaustausch", „Konfigurationen". Der Eintrag ist im Abschnitt „Router/Smtp", „Beschränkungen und Steuerungen", „SMTP Eingangssteuerung", „DNS-Blacklist-Filter" im Feld „DNS-Blacklist Sites" vorzunehmen. Es können mehrere Hostnamen getrennt durch Semikolon eingetragen werden. Identifiziert bereits einer der abgefragten Server den absendenden Server als potentiellen oder wirklichen Absender von Spam, wird die e-Mail als Spam angesehen. Darüber hinaus ist das Feld „DNS-Blacklist-Filter" auf „Aktiviert" zu setzen. Im Feld „Gewünschte

Aktion, wenn ein verbundener Host in einer DNS-Blacklist gefunden wurde“ ist eine der folgenden Aktionen auszuwählen:

- **„Nur protokollieren“**
  Eine e-Mail wird nicht zurückgewiesen; es erfolgt nur der Eintrag in der Protokolldatei „log.nsf“, dass die Mail von einem Blacklistet-Server kommt (eine gute Einstellung für die ersten Versuche!).

- **„Protokollieren und Nachricht markieren“**
  Eine e-Mail wird nicht zurückgewiesen; es erfolgt aber der Eintrag in der „log.nsf“ und das Datenfeld „$DNSBLSites“ wird der Mail hinzugefügt (diese Einstellung macht nur Sinn, wenn das Feld später über einen Agent o. Ä. ausgewertet wird).

- **„Protokollieren und Nachricht zurückweisen“**
  Eine e-Mail wird nicht angenommen, aber es erfolgt ein Eintrag in der „log.nsf“. Wird diese Option gewählt, sollte im Feld „Benutzerdefinierte Antwort auf SMTP-Fehler bei zurückgewiesenen Nachrichten“ ein sinnvoller Text eingegeben werden, der dem absendenden SMTP-Server mitteilt, warum seine e-Mail nicht angenommen wurde. Bleibt dieses Feld leer, wird die Standard-Nachricht „Connection denied based on policy reason“ gesendet.



Abfrage einer DNS Blacklist

Verhinderung von SMTP-Mail an Gruppen (ab R6)

Grundsätzlich ist es möglich, dass eine e-Mail aus dem Internet an Gruppen im primären oder einem der sekundären Adressbücher geschickt wird. Gibt es z.B. im Adressbuch einer Firma mit der Domäne „firma.de“ eine Gruppe „Alle“, die alle e-Mail Benutzer des Unternehmens enthält, dann könnte man aus dem Internet

eine beliebige Mail an alle@firma.de versenden. Noch unangenehmer ist die Tatsache, dass so eine e-Mail auch an Adressen außerhalb dieser Firma weitergeleitet würde. Gäbe es z.B. im Adressbuch eine Gruppe „Interessenten“, die die SMTP-Adressen aller Kunden-Interessenten enthält, dann könnte der Spammer über eine e-Mail an interessenten@firma.de diese alle erreichen.

Unterbinden kann man das Versenden der Mail an Gruppen im Adressbuch durch die folgende Zeile in „Notes.ini“ auf dem Domino-Server:

RouterDisableMailToGroups=1

Wirksam ist dieser Parameter nur für die e-Mail, die aus dem Internet (also von extern) kommt. Interne Lotus Notes- oder iNotes-Benutzer können weiterhin die Gruppen zur Mail-Adressierung heranziehen.

Tipp:
Manchmal werden Gruppen im Adressbuch für e-Mail-Adressen – wie z.B. info@firma.de oder verkauf@firma.de – verwendet. In diesem Fall muss vor der Aktivierung des Parameters für solche Adressen eine alternative Lösung gefunden werden, da diese ja nicht mehr von außen ansprechbar sind. Alternativen könnten eine „Mail-In-Datenbank“ sein oder ein zusätzliches Personendokument, das intern an die Gruppe weiterleitet.

Mail nur für Adressen im Adressbuch annehmen (ab R6)

Wird dem Domino-Server eine e-Mail über SMTP zugeschickt, dann nimmt er diese an und speichert sie in einer der mail.box-Dateien, vorausgesetzt die Domäne in der e-Mail-Adresse ist im „globalen Domänendokument" eingetragen. Erst danach wird im Adressbuch nachgeschaut, ob die Empfängeradresse im Adressbuch wirklich gefunden werden kann. Wird die Adresse nicht gefunden, geht die e-Mail an den Absender zurück, sofern dies technisch möglich ist.

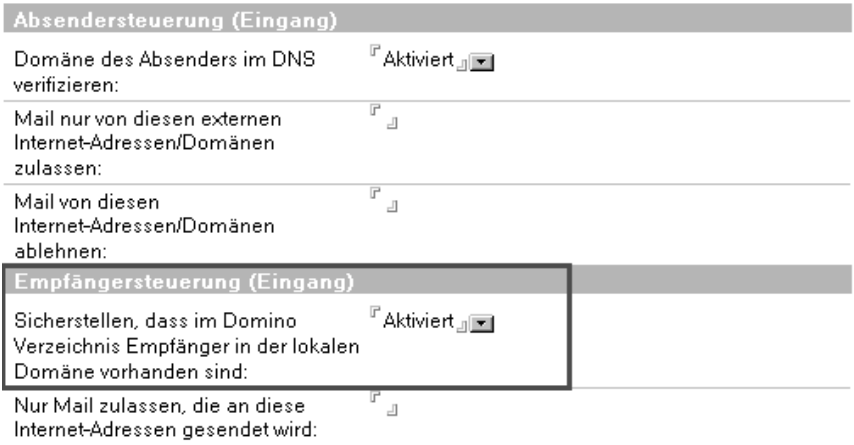
Häufig fälschen jedoch Spammer oder Virenversender die Absenderadresse. Je nachdem, ob die gefälschte Adresse wirklich existiert oder frei erfunden ist, führt dies entweder dazu, dass eine unzustellbare e-Mail entweder an jemanden zurückgesendet wird, der die Mail überhaupt nicht versendet hat, oder die e-Mail bleibt als „Dead" in der mail.box zurück. „Dead" bedeutet also, dass Domino die Mail weder dem vorgesehenen Empfänger zustellen noch an den Absender zurücksenden kann.

Ein konkretes Beispiel aus der jüngeren Vergangenheit: Ein Virus hat Tausende von Mails mit frei erfundenen Absendern an Adressen – wie aaaaa@firma.de, aaaab@firma.de, aaaac@firma.de usw. – versendet. Da solche Empfängeradressen i. d. R. nicht existieren, bleibt eine große Zahl von e-Mails als „Dead" in der mail.box hängen, da diese weder zugestellt noch an den nicht existierenden Absender zurückgesendet werden können.

Um solche „Dead"-Mails zu verhindern, kann Domino so konfiguriert werden, dass SMTP bereits während des Empfangvorgangs

prüft, ob die Empfängeradresse auch wirklich im primären oder einem der sekundären Adressbücher existiert.

Die entsprechende Einstellung wird im Domino-Verzeichnis (Datei „names.nsf“ auf dem Domino-Server) im Server-Konfigurationsdokument (vgl. Teil 2 Kapitel 4. 4. 1) vorgenommen. Das Konfigurationsdokument finden Sie in „Konfiguration“, „Nachrichtenaustausch“, „Konfigurationen“. Im Abschnitt „Router/Smtp“, „Beschränkungen und Steuerungen“, „SMTP Eingangssteuerung“, „Empfängersteuerung (Eingang)“ ist das Feld „Sicherstellen, dass im Domino-Verzeichnis Empfänger in der lokalen Domäne vorhanden sind:“ auf „Aktiviert“ zu setzen.



Mail nur für Adressen im Adressbuch annehmen

Tipp:
Bevor Sie diesen Parameter aktivieren, stellen Sie bitte sicher, dass das Feld „Internet-Adresse“ in allen

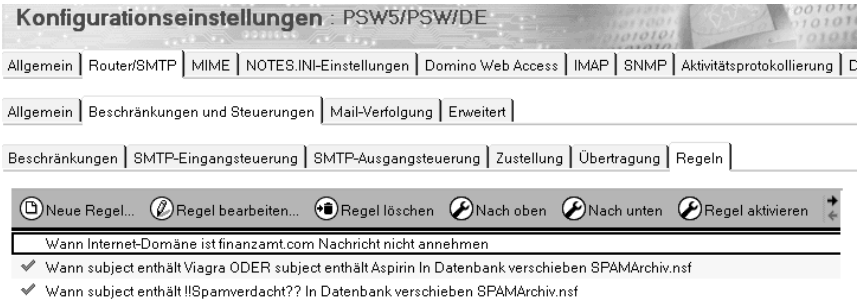
- Personendokumenten,
- Gruppendokumenten,
- Mail-In-Datenbank-Dokumenten

gepflegt ist, deren Adresse per SMTP-Mail erreichbar sein soll.

Server Mail-Regeln (ab R6)

Mail-Regeln bzw. QuickRules (vgl. Teil 1 Kapitel 4. 1. 8. 3) erlauben es dem Endbenutzer, eine gewisse Automatisierung der Verarbeitung von an ihn selbst gerichteten e-Mails zu erreichen. Mit den Server-Mail-Regeln steht dem Administrator ein ganz ähnlich zu handhabendes Werkzeug zur Verfügung, das ihm erlaubt, eine solche Automatisierung zentral zu erreichen.

Die entsprechenden Einstellungen werden im Domino-Verzeichnis (Datei „names.nsf“ auf dem Domino-Server) im Server-Konfigurationsdokument (vgl. Teil 2 Kapitel 4. 4. 1) vorgenommen. Das Konfigurationsdokument finden Sie in „Konfiguration“, „Nachrichtenaustausch“, „Konfigurationen“. Die Server-Regeln befinden Sich im Abschnitt „Router/Smtp“, „Beschränkungen und Steuerungen“, „Regeln“.



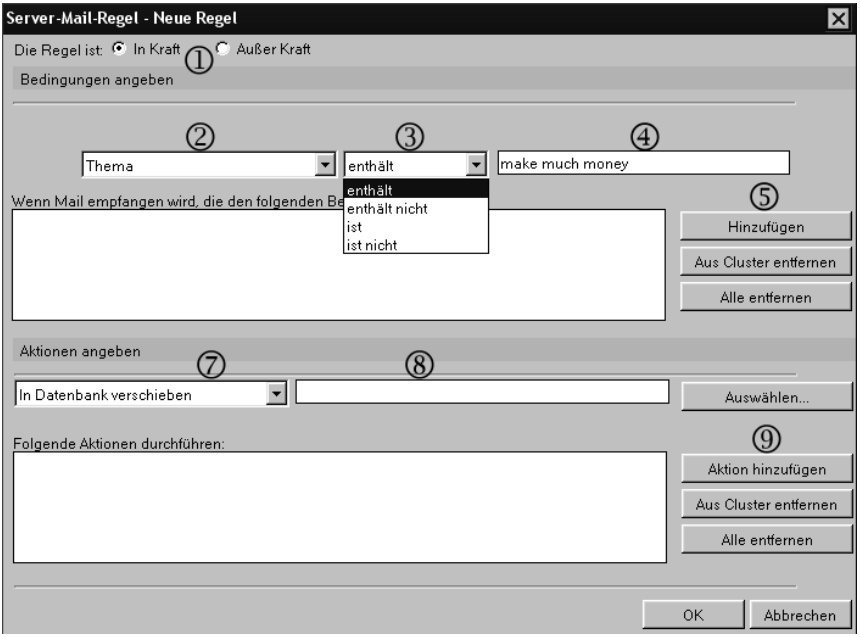
Server Mail-Regeln

Grundsätzlich werden durch die Mail-Regeln Aktionen für eingehende e-Mails festgelegt, die bestimmten Kriterien entsprechen. Der Mail-Router des Domino führt die festgelegten Regeln für **alle** Mails aus, die in der mail.box abgelegt werden. Die Regeln gelten also sowohl für SMTP als auch für Notes-Mail.

Eine Mail-Regel besteht aus drei einzelnen Definitionsabschnitten:

- der Definition der Bedingungen, auf die eingehende Mails geprüft werden
  - Vergleich von verschiedenen Bedingungen
  - unter Angabe unterschiedlicher Vergleichsoperanden
- die Angabe, welche der zuvor angegebenen Bedingungen erfüllt sein muss
  - Eine Bedingung muss zutreffen.
  - Alle Bedingungen müssen zutreffen.
- die auszuführende Aktion
  - Wie wird die Mail weiterverarbeitet.

Eine neue Mail-Regel wird durch Anklicken der Schaltfläche „Neue Regel…“ erstellt:



Neue Server-Mail-Regel

Im daraufhin angezeigten Fenster sind die drei Definitionsabschnitte auszufüllen:

- **Der allgemeine Bereich**
  1. Die Regel kann aktiviert („In Kraft“) bzw. deaktiviert („Außer Kraft“) werden.

- **Der Bedingungsbereich**

  2. Das zu prüfende Feld muss ausgewählt werden, z.B. Absender oder Thema (Betreff).
  3. Einer der Vergleichsoperatoren ist zu wählen.
  4. Der zu vergleichende Wert ist einzugeben.
  5. Die definierte Bedingung muss durch Klick auf „Hinzufügen“ übernommen werden.
  6. Bei Bedarf können die Schritte 2. - 5. mehrfach durchlaufen werden.
     Nach dem ersten Klick auf „Hinzufügen“ erscheint vor dem zu prüfenden Feld ein zusätzliches Feld, in dem durch Auswahl von „UND“ oder „ODER“ die festgelegten Bedingungen logisch verknüpft werden können.

- **Der Aktionsbereich**

  7. Die auf die ausgewählte Mail anzuwendende Aktion ist zu wählen.
  8. Je nach Aktion ist ein Zusatzparameter auszuwählen.
  9. Die definierte Aktion muss durch Klick auf „Aktion hinzufügen“ übernommen werden.
  10. Bei Bedarf können die Schritte 7. - 9. mehrfach durchlaufen werden.
      Alle ausgewählten Aktionen werden dann hintereinander ausgeführt.

Tipps:

In einem neuen Konfigurationsdokument können keine Mail-Regeln angelegt werden. Das Dokument muss erst gespeichert, geschlossen und neu geöffnet werden.

Da die Regeln von oben nach unten abgearbeitet werden, ist die Beachtung der Reihenfolge unter Umständen wichtig. Durch Anklicken einer Regel sowie durch Klick auf „Pfeil nach oben“ bzw. „Pfeil nach unten“ kann die Position einer Regel in Bezug auf die anderen Regeln geändert werden. Allerdings werden die Aktion(en) jeder Regel, deren Bedingung(en) für eine eingehende Mail zutreffen, ausgeführt.

Zur Prüfung in den Regeln können nur bestimmte Felder herangezogen werden. Der Zugriff auf alle Felder im Mail-Header ist leider nicht möglich. Hierdurch ergeben sich erhebliche Einschränkungen in der Flexibilität der Mail-Regeln. So ist es z. B. nicht möglich, die X-Felder auszuwerten, die oft von vorgeschalteten Virenschutz- oder Anti-Spam-Produkten zur Klassifizierung von e-Mails verwendet werden. Diese Produkte müssen so konfiguriert werden, dass die Klassifizierungsinfo z.B. in den Betreff (das Thema) einer e-Mail als Präfix eingebunden wird. Als Klassifizierungsinfo ist ein prägnanter Text denkbar wie z. B.: „!!Spam-Verdacht!!“.

Für Experten: Es ist möglich, über tiefes Eingreifen in den von Lotus/IBM gelieferten Code die Liste der prüfbaren Felder zu erweitern oder andere Änderungen bei den Mail-Regeln vorzunehmen („Hacking“). Da dieses Vorgehen aber dazu führt, dass ein so modifiziertes Domino-System von Lotus/IBM nicht mehr

supported ist, wird hier von einer Beschreibung der notwendigen Schritte abgesehen.

Aus der Liste der zu prüfenden Felder sind zwei Einträge erklärungsbedürftig:

- **„Beliebiger Empfänger“**
  Der Vergleichswert wird gegen den Inhalt aller Felder geprüft, die einen Empfänger enthalten können. Es handelt sich hierbei um die Felder „An“, „Kopie“ und „Blindkopie“.

- **„Alle Dokumente“**
  Die Regel trifft für jede eingehende Mail zu.

Der Vergleichswert ist immer ohne Anführungszeichen einzugeben. Werden Anführungszeichen verwendet, dann sind diese Bestandteil des Vergleichswertes; sie werden mitgeprüft. Die Anführungszeichen in den folgenden Beispielen dienen nur zur optischen Hervorhebung der Schlüsselworte.

Als Vergleichsoperatoren stehen zur Verfügung (beim Vergleich wird die Groß-/Kleinschreibung nicht beachtet):

- **„enthält“**
  Der eingegebene Vergleichswert muss irgendwo in dem verglichenen Feld vorkommen.
  Z.B. würde der Wert „viagra“ in einer Betreffzeile mit dem Inhalt „Buy Viagra cheap!“ gefunden; „enthält“ ist also der logische Ersatz des * für eine generische Suche. Würde als Vergleichswert „viagra*“ eingegeben, dann würde dieser Text in unserem Beispiel-Betreff nicht gefunden!

- **„enthält nicht“**
  Die Umkehrung von „enthält“.

- **„ist“**
  Der eingegebene Vergleichswert muss genau dem Inhalt des verglichenen Feldes entsprechen. Z.B. würde der Wert „viagra“ in einer Betreffzeile mit dem Inhalt „Buy Viagra cheap!“ **nicht** gefunden; man müsste stattdessen den gesamten Satz eingeben.

- **„ist nicht“**
  Die Umkehrung von „ist“.

Zur Auswahl stehen folgende Aktionen:

- **„Nachricht in Journal aufnehmen“**
  Führt dazu, dass die betreffende e-Mail in das Domino Mail-Journal übernommen (kopiert) und dem vorgesehenen Empfänger zugestellt wird. Diese Aktion kann dazu verwendet werden, alle oder bestimmte e-Mails in einer Notes-Datenbank zu protokollieren / archivieren.

- **„in Datenbank verschieben“**
  Die betreffende e-Mail wird in eine Notes-Datenbank verschoben. Durch Klick auf die Schaltfläche „Auswählen“ kann die Ziel-Datenbank ausgewählt werden. Die Datenbank muss bereits vorhanden sein und kann eine beliebige Struktur haben. Der vorgesehene Empfänger bekommt die e-Mail **nicht**. Mit dieser Aktion kann eine e-Mail z.B. in eine Quarantäne-Datenbank verschoben werden.

- **„Nachricht nicht annehmen“**
  Der Mail-Router nimmt die betreffende e-Mail überhaupt nicht an. Bei SMTP-Mail wird ein permanenter SMTP-Fehler an den absendenden Server zurückgemeldet, bei Notes-Mail erhält der Absender eine Nachricht über den Zustellfehlerbericht (NDR).

- **„Nachricht nicht zustellen“**
  Lässt den Mail-Router eine e-Mail zwar annehmen, aber nicht an den Empfänger zustellen. Es ist eine der beiden Zusatzoptionen „ungefragt löschen“ oder „Zustellfehlerbericht senden“ auszuwählen. „Ungefragt löschen“ führt zum unmittelbaren Löschen der eingegangenen Mail; bei „Zustellfehlerbericht senden“ wird eine e-Mail mit dem Hinweis auf die unterlassene Zustellung an den Absender gesendet.

- **„Routing-Status ändern“**
  Erfordert die Auswahl der Zusatzoption „als ‚zurückgehalten‘ markieren“. Hierdurch wird eine eingegangene e-Mail in der mail.box gehalten und nicht zugestellt. Erkennbar ist eine solche Mail an einem roten Ausrufezeichen in der ersten Spalte der Ansicht in der mail.box. Der Administrator kann dort diese Mail entweder löschen oder freigeben.

Verschlüsselte e-Mails werden nur insoweit geprüft, als dass die zu vergleichenden Werte in unverschlüsselten Feldern vorliegen (also nicht im Text der Mail).

Änderungen am Regelwerk können durch die Eingabe des folgenden Konsole-Befehls sofort aktiviert werden:

Set rules

Diese Seite ist zur Zeit nicht belegt.

9.8.2 Erfolgreicher mit Werkzeugen

Auch wenn mit den Bordmitteln von Domino gute Erfolge in der Bekämpfung von Spam erzielt werden können, ist doch der zu investierende Arbeitsaufwand hoch. Wie bei den einzelnen Parametern beschrieben, müssen die vorgenommenen Einstellungen regelmäßig überprüft bzw. überarbeitet werden. Einerseits müssen die gewählten Dienstleister (z.B. bei den Blacklists) daraufhin geprüft werden, ob sie überhaupt noch zur Verfügung stehen, andererseits macht es die große Kreativität der Spam-Versender erforderlich, zusätzliche Regeln zu erstellen oder zu ändern. Manche Parameter erfordern ein tiefes Verständnis der Arbeitsweise der Spammer (z.B. bei den Blacklists). Manche können dazu führen, dass auch eine unbedenkliche e-Mail abgewiesen wird (z.B. bei Reverse Lookup). Dann bekommt der Administrator den Unmut seiner Anwender zu spüren.

Effektiver und wirtschaftlicher ist sicherlich der Einsatz eines professionellen Werkzeuges.

Im Folgenden werden kostenlose bzw. preiswerte Lösungen beschrieben, die zu einer wesentlichen Reduktion des Spam-Aufkommens führen können. In Bezug auf die Trefferquote und der „False Positive“-Rate gibt es sicherlich leistungsfähigere Produkte, deren Einführung aber ein weitaus höheres Budget erfordert.

Scanmail Suite for Lotus Notes von TrendMicro

„Scanmail for Lotus Notes“ ist ein verbreitetes Werkzeug zur Bekämpfung von Viren im Notes-Umfeld. Verbreitet wohl auch deshalb, weil es fast alle Plattformen unterstützt, auf denen Domino läuft (z.B. Windows, iSeries).

Zusammen mit dem „eManager“ zur Spam-Abwehr und für die allgemeine Prüfung der e-Mail-Inhalte wird Scanmail ab Release 2.6 als „Scanmail Suite for Lotus Notes“ angeboten.

Der „eManager“ arbeitet zur Spam-Abwehr Datenbank-basiert und kann durch selbstdefinierte Regeln zur Inhaltsprüfung erweitert werden. So wie die Viren-Signaturen automatisch aktualisiert werden, findet ebenso die Aktualisierung der Datenbank durch Hinzufügen von Anti-Spam-Regeln statt. Diese Ergänzungen werden erfahrungsgemäß mehrmals täglich zur Verfügung gestellt. Sollte der „eManager“ eine Spam-Mail „übersehen“, kann der Kunde diese Mail an den Support von TrendMicro weiterleiten. Nach Prüfung wird dann gegebenenfalls eine Abwehrregel entwickelt, die dann per regelmäßiges Update allen Kunden zugestellt wird.

Umfangreiche Einstellungsmöglichkeiten, z. B. was mit einer als Spam klassifizierten e-Mail gemacht werden soll und wer in einem solchen Fall eine Nachricht erhalten soll, erlauben es dem Administrator, die Funktionsweise des „eManager“ den betrieblichen Notwendigkeiten anzupassen.

Der „eManager“ hat sich bisher als zuverlässiges Produkt mit einer ordentlichen Trefferquote bei einer sehr geringen Fehlalarm-Quote dargestellt.

Das Open Source-Projekt SpamAssassin (in verschieden Implementierungen)

Wichtiger Hinweis:
Der Name SpamAssassin ist als Warenzeichen für die amerikanische Firma Deersoft Inc. geschützt, die eine kommerzielle Version des Open Source-Projektes herstellt. Im Folgenden ist mit SpamAssassin immer das Open Source-Projekt SpamAssassin gemeint.

SpamAssassin ist ein erfolgreiches Open Source-Projekt, das nicht zu unrecht als eines der wichtigsten Werkzeuge zur Spam-Abwehr gilt. SpamAssassin setzt unterschiedliche Techniken ein, um Spam zu identifizieren. Im Wesentlichen lassen sich die durchgeführten Tests wie folgt kategorisieren:

- **Mail Header Analyse**
  Spammer versuchen, Ihre Identität zu verschleiern, indem anscheinend gültige Absenderadressen verwendet werden oder Adressen angegeben werden, die beim Empfänger den Eindruck erwecken, er hätte einen interessanten Newsletter abonniert. Solche Techniken versucht SpamAssassin zu entdecken.

- **Textanalyse**
  Spam enthält oft charakteristische Merkmale, wie z.B. die Tatsache, dass die gesamte Mail nur aus einer Grafik besteht oder aus Textpassagen in Großbuchstaben. Auch solche Charakteristika kann SpamAssassin erkennen.

- **DNS Blacklists**
  SpamAssassin kann mehrere Blacklist-Server anfragen, ob eine Mail von einem Mail-Server versendet wurde, der bereits an-

dere Spam versendet hat oder der technisch geeignet ist, Spam weiterzuleiten.

- **Spam-Datenbanken**
  Auch kann SpamAssassin im Internet öffentlich zugängliche Spam-Datenbanken anfragen, um festzustellen, ob die geprüfte Mail bereits von jemand anderem als Spam eingestuft wurde.

Im zurzeit aktuellen Release 2.6x wird jede e-Mail gegen ca. 1.000 Tests geprüft, die in die oben genannten Kategorien fallen. Jeder Test liefert als Ergebnis einen positiven oder einen negativen Punktwert. Ein positiver Wert wird geliefert, wenn es sich um ein Kriterium handelt, das typischerweise in einer unbedenklichen Mail gefunden wird, ein negativer, wenn das Kriterium auf eine Spam hinweist. Alle Punktwerte werden addiert und führen zu einer Bewertungszahl für die geprüfte e-Mail. Je niedriger diese Punktzahl ist, desto unwahrscheinlicher ist es, dass eine Mail eine Spam-Mail ist. Überschreitet die Punktzahl einen vom Administrator festgelegten Schwellwert, wird die Mail als Spam eingestuft. In einem solchen Fall werden die ermittelte Punktzahl und andere Informationen in Mail-Header-Feldern (X-Header) in der geprüften e-Mail dokumentiert und optional wird ein definierbares Schlüsselwort in den Betreff eingefügt. Anhand dieses Schlüsselwortes könnte im Mail-Programm des Empfängers (eventuell automatisiert durch QuickRules) entschieden werden, was mit der Mail geschehen soll.

SpamAssassin benötigt wenig Administration. Im Wesentlichen sind nur der Schwellwert festzulegen und gegebenenfalls das Schlüsselwort für den Betreff. Beachtet werden sollte allerdings, dass wegen der hohen Dynamik im Spam-Umfeld SpamAssassin

regelmäßig aktualisiert werden muss. In jedem neuen Release sind neue Tests integriert – oder Prüfungen werden so aktualisiert, dass z.B. keine Datenquellen angesprochen werden, die im Internet nicht mehr zur Verfügung stehen.

Da 1.000 Tests pro e-Mail eine erhebliche Prozessor-Belastung sein können, ist diese Tatsache bei der Auswahl des Rechners zu berücksichtigen, auf dem SpamAssassin installiert werden soll.

Als Open Source-Produkt liegt es natürlich nahe, SpamAssassin auf einem Linux-Rechner zu installieren, der dem bestehenden Domino vorgeschaltet wird. Wegen der hiermit verbundenen hohen Implementierungs- und Supportkosten ist diese Vorgehensweise für viele Unternehmen wirtschaftlich zumindest fragwürdig – dies insbesondere, weil SpamAssassin regelmäßig aktualisiert werden sollte.

Gerade in kleineren Unternehmen (bis zu ca. 120 Benutzer) mag die Implementierung von SpamAssassin als Bestandteil einer so genannten Internet-Access Appliance interessant sein. Solch eine Appliance ist eine „Black-Box“, die aus einem PC in einem speziellen Gehäuse mit Linux-Betriebssystem besteht. Diese Geräte verfügen weder über Bildschirm noch Tastatur, werden weitgehend vorkonfiguriert geliefert und über einen Internet-Browser einfach und schnell konfiguriert. Üblicherweise ist eine Menge von Funktionen implementiert: ISDN- oder DSl-Router, Firewall, Virenfilter, URL-Filter, Proxy, Spam-Filter mit SpamAssassin und vieles andere mehr. Im Rahmen eines Wartungsvertrages sind professioneller Support sowie regelmäßige Updates kein Problem. Beispiele für solche Appliances sind die „TuxGate“ von CompuShack Production und der „BenHur“ von Pyramid Computer.

Als unter Windows lauffähige Implementierung des SpamAssassin empfiehlt sich das Produkt No-Spam-Today von Paessler Software. Durch Starten eines einfachen Installationsprogramms lässt sich No-Spam-Today in Minuten installieren oder ebenso einfach ein neues Release einspielen. Die einfache Konfiguration macht das Produkt in kürzester Zeit einsatzbereit. Unterstützt werden zwei Implementierungsarten: entweder direkt auf demselben Rechner wie Domino (natürlich nur sofern es auf einem Rechner mit Windows-Betriebssystem installiert ist) oder separat auf einem anderen Rechner, der zwischen Domino und Internet geschaltet wird. Die Installation zusätzlich zu Domino auf demselben Rechner ist aus Performance- und Sicherheitsgründen nur dann empfehlenswert, wenn in einem Unternehmen zwei Domino-Server eingesetzt werden: der eine als Haupt-Server im internen Netz und der zweite als Mail-Relay – z.B. in einer DMZ. Da die Performance auf dem als Mail-Relay fungierenden Domino meist kein Problem ist, wäre hier No-Spam-Today ideal untergebracht. Die Installation auf einem separaten Rechner macht dann Sinn, wenn nur ein Domino vorhanden ist oder dieser auf einer nicht Windows-Plattform läuft, wie z.B. der iSeries. Auch bei diesem Produkt sind professioneller Support und regelmäßige Updates selbstverständlich.

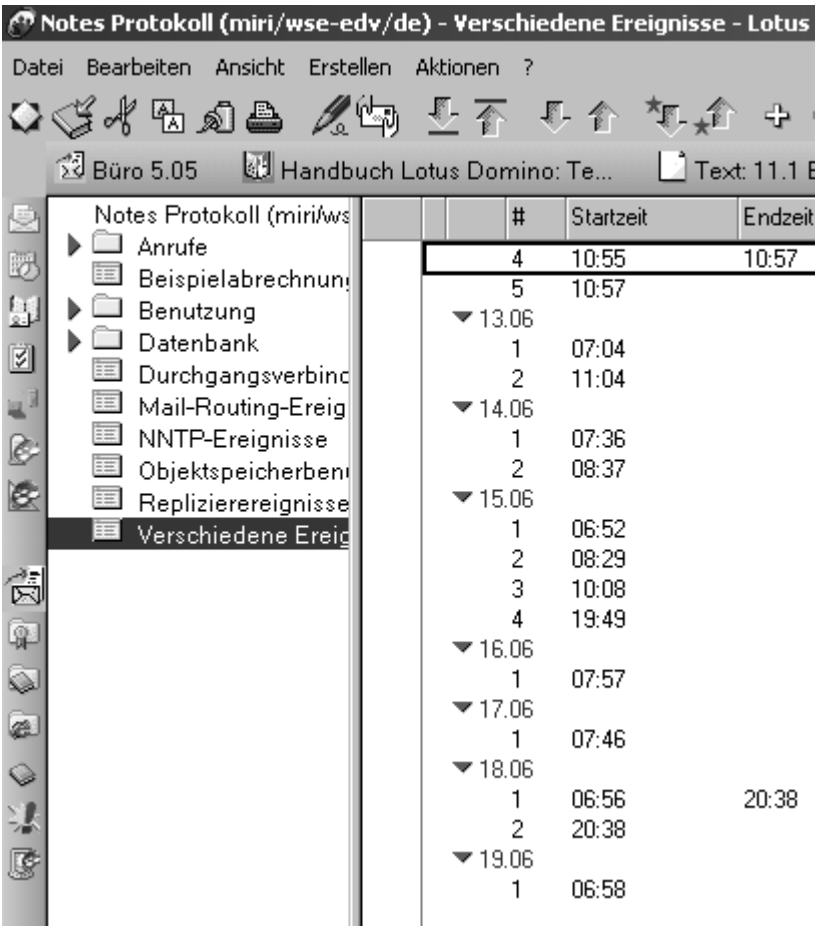
11

Statistikdaten und Auswertungen

Lotus Domino als Client-/Server-System in heterogenen Netzwerken verfügt als Hilfsmittel für den Administrator über zahlreiche Systemaufzeichnungen, in denen Daten über Fehler, Ausnahmefälle und auch die Ausführung bestimmter Aktionen (wie z. B. die Weiterleitung von e-Mails). Darüber hinaus werden aber auch Systemwerte festgehalten und es ist möglich, die unterschiedlichsten Ereignisse in speziellen Datenbanken und Reports zu protokollieren.

August 2001 / 6. EL

Die Standard-Datenbank für Meldungen und Informationen über die Arbeit der Server ist die Datenbank „log.nsf“. Hier werden, je nach angegebener Aufzeichnungsart, alle Informationen gesammelt, die auch an der Konsole angezeigt werden.



Die Datenbank Log.nsf

Für die Erstellung der Auswertungen sind Server-Prozesse zuständig, die automatisch gestartet werden. Sie sammeln sowohl Statistikwerte als auch Ereignisse und speichern sie in die entsprechenden Datenbanken. So werden z. B. über den Prozess „Collect“ Daten in die Datenbank „STATREP.NSF“ gestellt.

Der Prozess „Collect“

Über so genannte Monitor-Dokumente können Grenzwerte festgelegt werden, die dazu führen, dass in der Datenbank „STATREP.NSF“ ein Alarmbericht erstellt wird, sobald eine Überschreitung dieser Grenzwerte festgestellt wird.

Diese Seite ist zur Zeit nicht belegt.

11.1 Berichtsdaten sammeln und Statistik-Dokumente konfigurieren

Während die Daten der Datenbank „log.nsf" automatisch erstellt werden, müssen für die weiteren Datenbanken zum Teil Einträge in Steuerdokumenten vorgenommen und Datenbanken erstellt werden. Lotus versucht dabei immer mehr, auch die erforderlichen Prozesse und Datenbanken für Statistiken standardmäßig zu erstellen, zu starten und über Vorgabewerte zu steuern.

Die Erstellung von Statistikdaten übernehmen die Server-Prozesse Event, Collect, mtc usw. Sie werden über die Datei „notes.ini" gestartet und nehmen ihre Arbeit zu den angegebenen Uhrzeiten auf, soweit sie nicht die komplette Server-Laufzeit über aktiv sind. Die Einträge in der Datei „notes.ini" können z. B. folgendermaßen aussehen:

```
ServerTasks=Router,Replica,Update,Amgr,AdminP,
      CalConn,Event,Sched,Stats,HTTP,DIIOP,DECS
ServerTasksAt1=Catalog,Design
ServerTasksAt2=UpdAll,Object Collect mailobj.nsf
ServerTasksAt3=Object Info -Full
ServerTasksAt5=Statlog
```

Dabei werden die Prozesse des Eintrags „ServerTasks" mit dem Server gestartet und arbeiten in regelmäßigen Abständen. Die Prozesse der Einträge „ServerTasksAt1" bis „ServerTasksAt5" werden zu der hinter „At" stehenden Uhrzeit gestartet und nach Ausführung ihrer Aufgabe wieder beendet. So wird bei dem Server im obigen Beispiel der Prozess „UpdAll" um 2.00 Uhr nachts gestartet.

Diese Seite ist zur Zeit nicht belegt.

11.1.1 Die Datenbank „log.nsf“

Der Inhalt der Datenbank „log.nsf“ hängt sehr eng mit der Konsolanzeige zusammen. Es werden alle Ereignisse gespeichert, die auch an der Konsole angezeigt werden. Die Datenbank wird automatisch zusammen mit dem Server angelegt und findet sich im Datenverzeichnis dieses Servers. Welche Daten gespeichert werden, hängt von den Einträgen in der Datei „notes.ini“ ab, von denen die Konsolanzeige gesteuert wird. Der Grundeintrag heißt „Log“. Die Syntax dieses Wertes lautet:

log = Name der Datenbank, Option, Nicht verwendet, Tage, Größe

Dabei bedeutet:

Name der Datenbank
Normalerweise heißt die Protokolldatenbank „log.nsf“.
Sie kann aber auch einen anderen Namen erhalten.

Option
Hier können folgende Werte eingetragen werden:

1 = An der Konsole protokollieren

2 = Datenbank-FixUp beim Öffnen der Protokolldatei erzwingen

4 = Vollständige Dokumentprüfung

Nicht verwendet
Dieser Parameter wird zur Zeit nicht verwendet.

Tage
Anzahl der Tage, für die Protokolldokumente aufbewahrt werden.

Größe
Maximale Größe der einzelnen Protokoll-Dokumente

Ein üblicher Eintrag sieht etwa so aus:

log=log.nsf, 1, 0, 7, 40000

Er bewirkt:

- dass die Protokollierung in die Datenbank „log.nsf“ erfolgt, dass sie an der Konsole angezeigt wird,
- dass Dokumente, die älter als 7 Tage sind, gelöscht werden dass die Texte der Ereignisdokumente nicht länger werden als 40 000 Zeichen.

Weitere Einträge sind:

Log_AgentManager
Wird dieser Eintrag mit 1 oder 2 angegeben, so wird die Ausführung von Agenten protokolliert.

Beispiel: Log_AgentManager=2

Dieser Eintrag bewirkt, dass nur solche Agenten protokolliert werden, die erfolgreich ausgeführt wurden.

Log_DirCat
Damit werden Informationen zu dem Prozess „Directory Cataloger“ aufgezeichnet (Startzeit, Aufzeichnungsverzeichnisse, Beendigungszeitpunkt).

Beispiel: Log_DirCat=1

Es werden Informationen zum Directory Cataloger vorgenommen.

Log_Replication
Je nach eingetragenem Wert werden Informationen zum Verlauf von Datenbankreplikationen aufgezeichnet:

0 = keine Aufzeichnung von Replikationsinformationen

1 = nur Server-Replikation überwachen

2 = Replikation auf der Ebene der Datenbanken protokollieren

3 = Replikation auf der Ebene der Datenbankelemente (Ansichten, Dokumente usw.) protokollieren

4 = Informationen über die Replikation bis hin zu Feldern aufzeichnen

5 = zusammenfassende Informationen dokumentieren

Beispiel: Log_Replication=0

Es wird keine Protokollierung von Replikationsvorgängen vorgenommen.

Log_Sessions
Benutzer-Sitzungen werden über diesen Eintrag ebenfalls protokolliert.

Beispiel: Log_Sessions=1

Auch für Benutzersitzungen werden Informationen aufgezeichnet.

Log_Tasks
Über die Werte 0 oder 1 wird gesteuert, ob der Status der Prozesse ebenfalls protokolliert wird.

Beispiel: Log_Tasks=1

In die Protokolldatenbank werden auch Statusinformationen zu Server-Prozessen aufgenommen.

Log_Update
Protokolliert Ereignisse zum Indexer-Prozess:

0 = Nur Beginn und Ende werden aufgezeichnet

1 = Die indizierten Datenbanken werden zusätzlich angegeben

2 = Auch die indizierten Ansichten werden genannt

Beispiel: Log_Update=2

Mit diesem Eintrag wird eine ausführliche Protokollierung des Indexer-Prozesses erreicht.

Log_View_Events
Protokolliert Ereignisse beim Neuaufbau von Ansichten.

Beispiel: Log_View_Events=0

Beim Erstellen von Ansichten erfolgt keine Protokollierung.

Mail_Log_To_Miscevents
Über 0 oder 1 wird festgelegt, ob alle Mail-Ereignisse protokolliert und in der Ansicht „Verschiedene Ereignisse“ angezeigt werden.

Beispiel: Mail_Log_To_Miscevents=1

Mail-Ereignisse werden in der Datei “log.nsf” aufgezeichnet und angezeigt.

No_Force_Activity_Logging
Steuert, ob der Prozess „StatLog“ die Aufzeichnung von Datenbankaktivitäten aktiviert.

No_Force_Activity_Logging=1

Die automatische Protokollierung von Datenbankaktivitäten wird nicht aktiviert.

Passthru_LogLevel
Dieser Eintrag steuert den Umfang der Protokollierung für Netzwerkverbindungen.

0 = Keine Protokollierung.

1 = Nur Fehler werden aufgezeichnet.

2 = Es werden Kurzinformationen aufgezeichnet.

3 = Detailinformationen werden gespeichert.

4 = Alle Informationen werden eingetragen.

5 = Zu den Grundinformationen werden zusätzlich Treibermeldungen aufgezeichnet.

Beispiel: Passthru_LogLevel=1

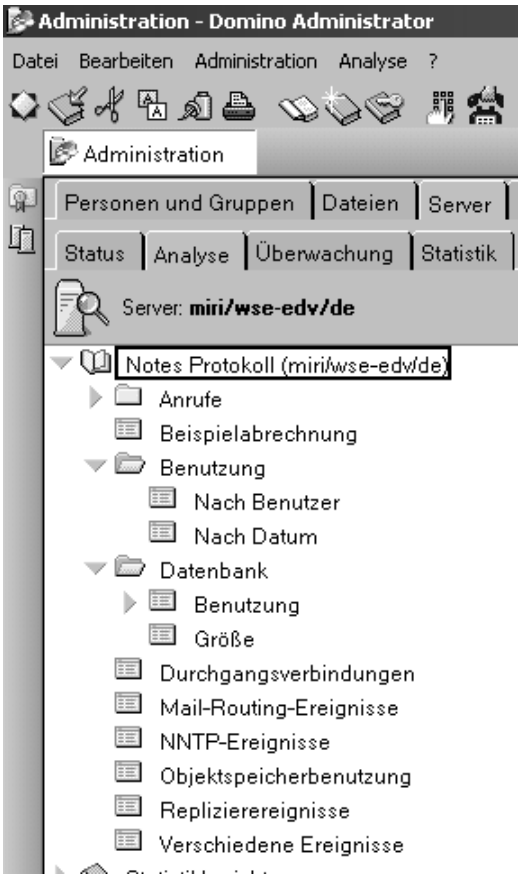
Fehlermeldungen bei Netzwerkverbindungen werden im Protokoll des Servers aufgezeichnet.

PhoneLog
Über die Werte 0 bis 2 wird gesteuert, ob und in welchem Umfang Telefonanrufe des Servers in der Protokolldatei gespeichert werden.

Beispiel: PhoneLog=2

Alle Telefonanrufe werden protokolliert.

Die gespeicherten Protokollinformationen können über den Administrator-Client oder in der Datenbank “log.nsf” direkt angezeigt werden.



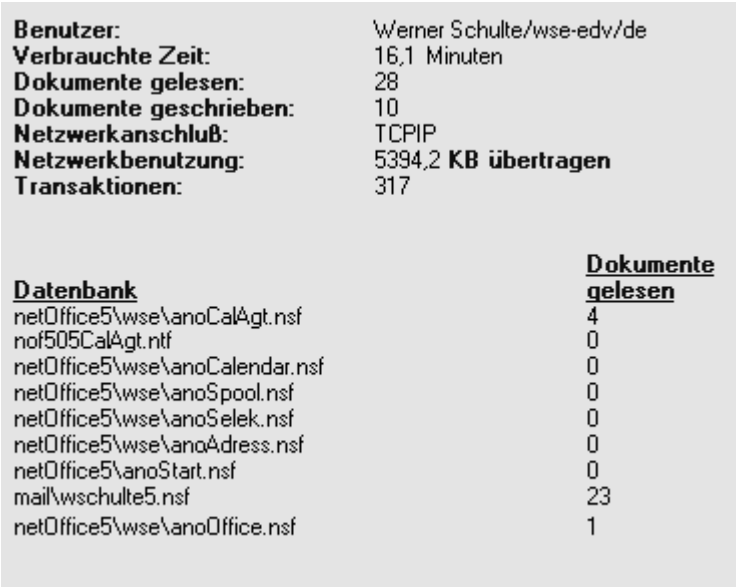
Notes-Protokoll

In den verschiedenen Ansichten werden Ausschnitte der Protokolldokumente angezeigt.

Benutzer	Datum	Uhrzeit	Minuten	Lesezugriffe
▶ ann/wse-edv/de			1	2
▼ Werner Schulte/wse-edv/de			12330	50372
	▶ 12.05		0	6
	▶ 13.05		198	57
	▶ 14.05		357	34150
	▶ 15.05		641	508
	▶ 16.05		722	4085
	▶ 17.05		1069	1306
	▶ 18.05		621	163
	▶ 19.05		409	163
	▶ 20.05		80	51
	▶ 21.05		962	572
	▶ 22.05		667	243
	▶ 23.05		557	231
	▶ 24.05		376	144
	▶ 08.06		145	193
	▶ 09.06		407	218
	▶ 10.06		34	9
	▼ 11.06		769	273
		07:08	212	77
		07:08	0	1

Ansicht Benutzung

Die Dokumente selbst enthalten die Meldungen, die während ihrer Erstellung aufgezeichnet wurden.



Benutzer:	Werner Schulte/wse-edv/de
Verbrauchte Zeit:	16,1 Minuten
Dokumente gelesen:	28
Dokumente geschrieben:	10
Netzwerkanschluß:	TCPIP
Netzwerkbenutzung:	5394,2 **KB übertragen**
Transaktionen:	317

Datenbank	**Dokumente gelesen**
netOffice5\wse\anoCalAgt.nsf	4
nof505CalAgt.ntf	0
netOffice5\wse\anoCalendar.nsf	0
netOffice5\wse\anoSpool.nsf	0
netOffice5\wse\anoSelek.nsf	0
netOffice5\wse\anoAdress.nsf	0
netOffice5\anoStart.nsf	0
mail\wschulte5.nsf	23
netOffice5\wse\anoOffice.nsf	1

Dokument zu Benutzeraktivitäten

Folgende Ansichten geben Auskunft über protokollierte Informationen:

- Anrufe
- Anzeige der Telefonanrufe des Servers nach Benutzer oder Datum
- Beispielabrechnungen
- Kostenerfassungsinformationen

- Benutzung nach Benutzer oder Datum
- Datenbanken nach Benutzung oder Größe
- Die Ansicht der Datenbanken nach Größe zeigt auf den ersten Blick, welches die Datenbank mit dem höchsten Platzverbrauch ist.

#	Datenbank	Größe (KB)	% belegt	Wöchentliche Benutzung
▼ miri/wse-edv/de		4.237.533	84	3736
1	Midrangemagazin	605.952	100	37
2	Lotus Domino Handbuch - Teil I	576.256	13	41
3	Werner Schulte	471.552	100	591
4	netOffice 5 Arbeitsplatz	393.984	99	76
5	netOffice 5 Adressen	331.008	98	1
6	netOffice 5 Adressen	330.752	97	2
7	Import	179.200	68	6
8	Import	154.624	20	3
9	netOffice 5 Selektierte Adresser	50.432	60	1
10	netOffice 5 Selektierte Adresser	50.432	61	1
11	Admin Stoffsammlung 5.1	36.864	93	1
12	Handbuch Lotus Domino: Teil II	35.840	97	13
13	Admin-Stoffsammlung Neu	32.768	100	0
14	Entwicklung Handbuch 5.1	30.464	99	1
15	Entwicklung Stoffsammlung 5.1	29.696	98	0
16	Entwicklung Folien 5.1	29.184	95	6
17	Domino 5 Designer Hilfe	28.416	98	0
18	Programmiersprachen	28.160	98	11

Datenbanken eines Servers nach Größe

In den Datenbankdokumenten wird außerdem gezeigt, welcher Plattenplatz durch Komprimierung gewonnen werden kann.

```
13.06.2001 11:04:38  Agent Manager gestartet
13.06.2001 11:04:41  AMgr: Executive '1' gestartet
13.06.2001 11:04:43  miri/wse-edv/de ist der Administrationsserver des Domino Verzeichnisses.
13.06.2001 11:04:43  Administrationsprozeß gestartet
13.06.2001 11:04:48  Calendar Connector gestartet
13.06.2001 11:04:53  Ereignis-Monitor gestartet
13.06.2001 11:04:57  Schedule Manager gestartet
13.06.2001 11:04:58  SchedMgr: Validieren der Planungsdatenbank
13.06.2001 11:05:00  AMgr: Agent ('getAppointments' in 'netOffice5\wse\anoCalAgt.nsf') gibt aus:
13.06.2001 11:05:03  Stats Agent gestartet
13.06.2001 11:05:21  SchedMgr: Validieren der Planungsdatenbank abgeschlossen
13.06.2001 11:05:24  Datenbankserver gestartet
13.06.2001 11:05:25  DIIOP-Server auf miri gestartet
13.06.2001 11:05:27  DECS Server started
13.06.2001 11:05:29  JVM: Java Virtual Machine initialisiert.
13.06.2001 11:05:29  Directory Cataloger wird gestartet
13.06.2001 11:05:35  AMgr: Agent ('getAppointments' in 'netOffice5\wse\anoCalAgt.nsf') gibt aus:
13.06.2001 11:05:57  HTTP Web Server started
13.06.2001 11:10:38  Datenbank 'Administrationsanfragen' suchen.
13.06.2001 11:15:01  AMgr: Agent ('getAppointments' in 'netOffice5\wse\anoCalAgt.nsf') gibt aus:
```

Datenbank-Daten

Durch Komprimieren der einzelnen Datenbanken oder durch Ausführung des Prozesses „Compact“ mit dem Server-Befehl „Load Compact“ wird der nicht benutzte Speicherplatz in den Datenbanken wieder freigegeben.

- Durchgangsverbindungen
- Mailrouting-Ereignisse
  Meldungen zur Verarbeitung von e-Mails durch den Server.
- NNTP-Ereignisse
  Informationen, die bei der Verbindung mit News-Servern entstehen.

- Objektspeicherbenutzung
- Replizierereignisse
- Verschiedene Ereignisse

Meldungen, die in anderen Ansichten nicht gezeigt werden.

Lotus Domino Handbuch -

Pfadname:	Doku\LDR5 Handbuch Praxis\PraxisHandbuch.nsf	
Dateigröße:	562,8 Mbytes (12,60% dieses Speicherplatzes ist belegt)	
Größe der Ansichten:	Alle Dokumente	207 Kbytes
	(Book Autor)	0 Kbytes
	(Book Bearbeiten)	322 Kbytes
	(Book Buchart)	0 Kbytes
	(Book Buchtitel)	10 Kbytes
	(Book Buecher)	45 Kbytes
	(Book Datum)	0 Kbytes
	(Book Inhalt)	10 Kbytes
	(Book Präsentation)	0 Kbytes
	(Book Projekt)	0 Kbytes
	(Book Suchbegriff)	0 Kbytes
	(Book Themen)	0 Kbytes
	(Book Zuständig)	0 Kbytes
	(Dokumente nach Seitennummer)	0 Kbytes
	(Hilfe)	0 Kbytes
	(Kat Buchart)	0 Kbytes
	(Kat Buch)	9 Kbytes
	(Kat Categories)	9 Kbytes
	(Kat FolgeAktion)	0 Kbytes
	(Kat Kapitel nach Nummer)	0 Kbytes
	(Kat Kapitel)	0 Kbytes
	(Kat Projekt)	0 Kbytes
	(Kat Sachgebiet nur Nummer)	0 Kbytes
	(Kat Sachgebiet)	0 Kbytes
	(Kat SuchKapitel)	0 Kbytes
	(Kat SuchSachgebiet)	0 Kbytes
	(Texte - DocId)	0 Kbytes
	(Texte nach Name)	0 Kbytes

Manager:
WSE-Development
Administratoren
Werner Schulte/wse-edv/de
Werner Schulte/WSE3/de

Verschiedene Ereignisse

Das Notes-Protokoll eines Servers ist oft die erste Informationsquelle, wenn es darum geht, Probleme im Domino-System zu lösen.

11.2 Performance im Domino-System

"Warum dauert denn das wieder so lange?" Das hat sich sicher jeder Anwender irgendwann schon einmal gefragt. Wer aber nach Ursachen für Engpässe im Bereich Performance sucht, wird gerade beim Lotus Domino Server und dessen Lotus Notes Client oft nur vage Aussagen und unbefriedigende Antworten erhalten. Schuld daran ist die Komplexität des Zusammenspiels der verschiedenen Komponenten in Domino-Systemen.

Wenn man solche Systeme anschaut, sind es im Wesentlichen folgende Faktoren, die zu einer Installation von Lotus Notes Clients und Lotus Domino Servern gehören und die Einfluss auf die Antwortzeiten nehmen:

- unterschiedliche Varianten von Programmen auf der Client-Seite (Lotus Notes Client, Web-Browser, POP3-Client, IMAP-Client)
- die Hardware auf der Client-Seite
- unterschiedliche Verbindungen vom Lotus Notes Client zum Lotus Domino Server (Modem direkt, Internet, Netzwerk)
- die technischen Eigenschaften des installierten Netzwerkes
- die Anzahl der Benutzer und die Anwendungen, die von den Benutzern eingesetzt werden (e-Mail, Notes-Datenbanken, Web-Seiten usw.)
- die verschiedenen Hardware- und Betriebssystem-Plattformen, für die der Lotus Domino Server verfügbar ist (iSeries/400 mit OS/400, AMD oder Intel-Systeme mit Linux oder Windows 2000 usw.)

August 2001 / 6. EL

Dazu kommt, dass, so banal es auch klingen mag, Unternehmen und deren Arbeitsabläufe einer permanenten Veränderung unterworfen sind. Ein System, das heute noch ausreichend schnell Daten bereitstellt und e-Mails verteilt, kann morgen schon hoffnungslos überlastet sein. Bevor man also konkrete Angaben über die Performance machen oder gar Maßnahmen einleiten kann, ist zunächst eine genaue Analyse der bestehenden Domino-Installation erforderlich.

11.2.1 Dokumentieren der Systembasis

Die Grundlage für eine systematische Performance-Analyse bildet zunächst die Dokumentation der bestehenden Situation. Die hier ermittelten Werte können dann objektiv und genau passend zum spezifischen Lotus Domino Server verglichen werden. Bei der Dokumentation teilt sich die Betrachtung eines Lotus Domino Servers in zwei Teile auf:

- zum einen in die zur Verfügung stehende Hardware und das entsprechende Betriebssystem,
- zum anderen in die Konfiguration und Nutzung des Lotus Domino Servers selbst.

Auf allen Plattformen, auf denen der Lotus Domino Server zur Verfügung steht, bietet jedoch auch das Betriebssystem Möglichkeiten, um die Auslastung des Systems zu messen:

- WRKACTJOB, WRKSYSSTS oder WRKDOMSVR unter OS/400 auf dem iSeries/400
- mehrere grafische Werkzeuge unter Windows NT
- Task Manager (taskman.exe)
- Performance Monitor (perfmon.exe)
- Data Logging Service (datalog.exe)
- vmstat, netstat und perfmeter unter Linux/Solaris.

"Auf einem langsamen System wird kein schneller Lotus Domino Server laufen". Dieses Zitat stammt aus einer Publikation zum Thema Performance von IRIS (dem Bereich von IBM/Lotus, in

August 2001 / 6. EL

dem die Entwicklung von Notes und Domino betrieben wird) und dem ist kaum etwas hinzuzufügen. Wenn ein System zu schwach dimensioniert ist, um einen Lotus Domino Server darauf zu betreiben, dann hilft auch die beste Performance-Analyse des Servers und seiner Parameter nichts. Die Hauptkennzahlen, auf die man bei der Untersuchung des Grundsystems achten muss, sind:

- CPU-Auslastung
- Anzahl der Festplattenzugriffe
- Geschwindigkeit der Zugriffe
- Auslastung der Netzwerk-Adapter
- Auslastung des Netzwerks generell

Wichtig ist es, die oben aufgeführten Werte regelmäßig und automatisch zu protokollieren. Erst dadurch wird es möglich, zu erkennen, welcher Wert so stark angestiegen bzw. abgesunken ist, dass er die Performance des Gesamtsystems beeinflusst.

Unter Windows NT wird über das Resource Kit der "at"-Befehl geliefert, der es ermöglicht, die oben aufgeführten Werkzeuge automatisch und zeitmäßig zu steuern. Mit den Befehlen

at \\Beagle 9:00 /date:M,T,W,Th,F „monitor start"

at \\Beagle 12:00 /date:M,T,W,Th,F „monitor stop"

kann z. B. der Performance-Monitor gestartet und beendet werden.

Auf dem iSeries/400 sind nur die Programme für das Sammeln der Performance-Daten standardmäßig installiert. Für die Auswertung kann das Feature "Perfomance Tools for AS/400 (5769-

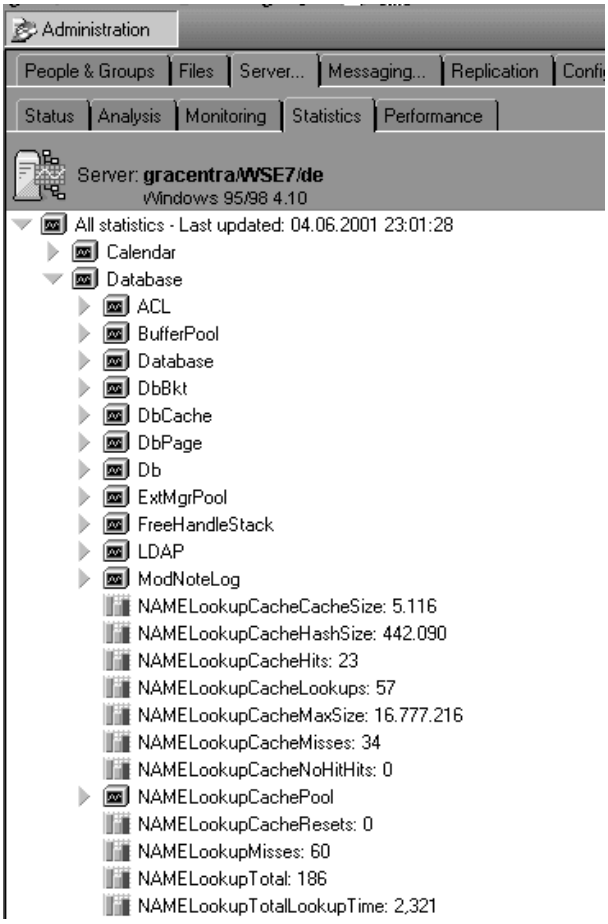
PT1)" verwendet werden. Mit dem Befehl STRPFRMON wird der Performance-Monitor gestartet. Bei Bedarf kann er ebenfalls zeitgesteuert über den Befehl ADDJOBSCDE automatisch zu bestimmten Zeiten gestartet und beendet werden.

Diese Seite ist zur Zeit nicht belegt.

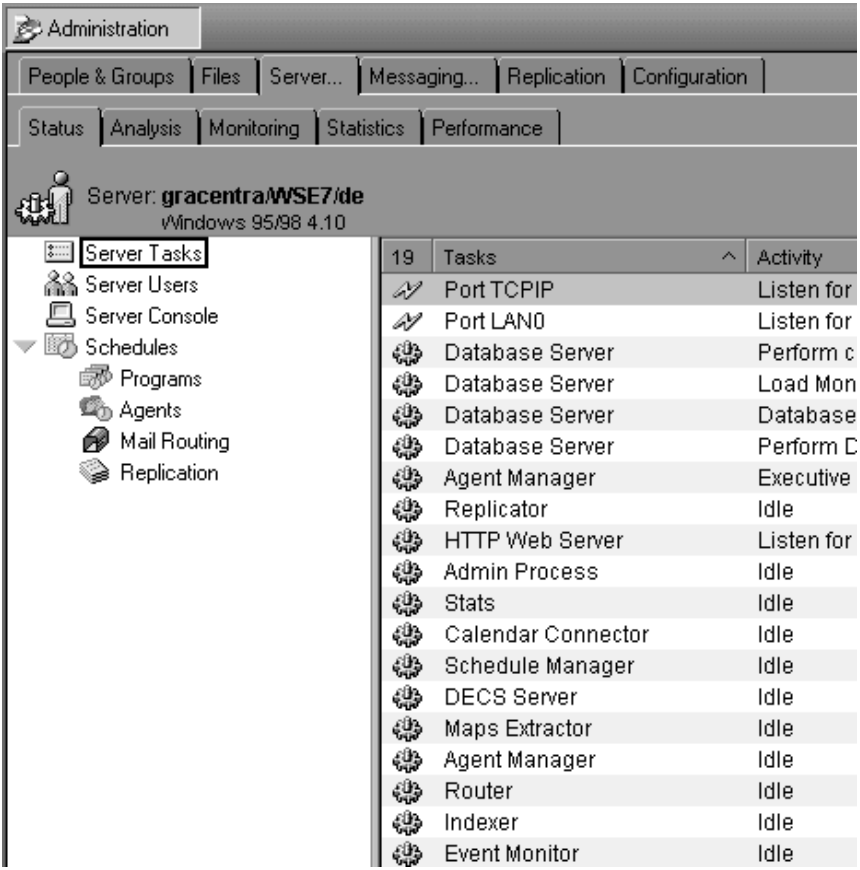
11.2.2 Analyse des Lotus Domino Servers

Über die Protokollierung und die Analyse auf Systemebene hinaus, kann als nächstes der Zustand des Lotus Domino Servers selbst betrachtet werden. Die zentrale Stelle hierfür ist seit dem Release 5 der Administrations-Client. Er bietet auf allen Betriebssystemversionen mehrere einheitliche Statistiken, Alarm- und Überwachungsmöglichkeiten.

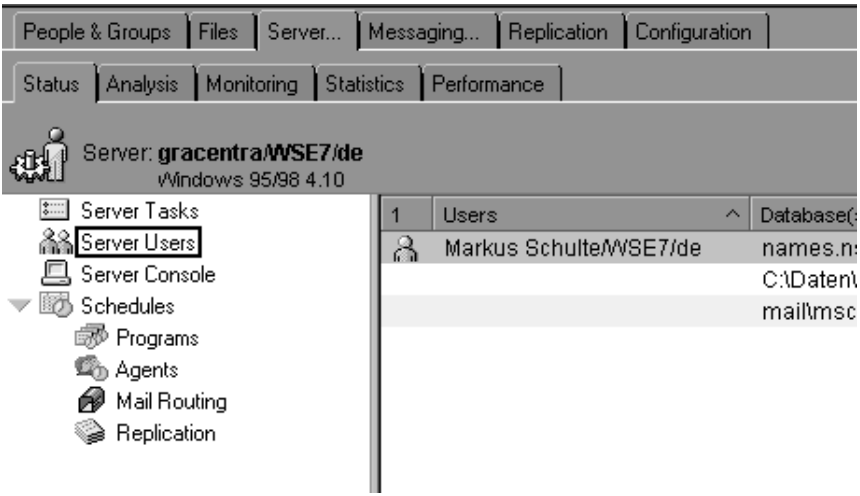
Die ermittelten Daten können sowohl direkt als auch nachträglich über einen Zeitraum hinweg ausgewertet werden. Das Spektrum reicht von der Übersicht über gerade aktive Tasks des Lotus Domino Servers oder gerade aktive Benutzer bis hin zu detaillierten Werten über die Umgebung, in der der Server läuft.



Übersicht aktive Tasks



Übersicht aktive Benutzer



Übersicht Statistikwerte

Die einzelnen Bereiche des Server-Registers sind:

- Status
- Analyse
- Monitoring
- Statistiken
- Performance

Hinter jedem dieser Register finden sich Anzeigen und Auswertungen zum aktuellen Server und seiner Umgebung.

11.2.2.1 Status

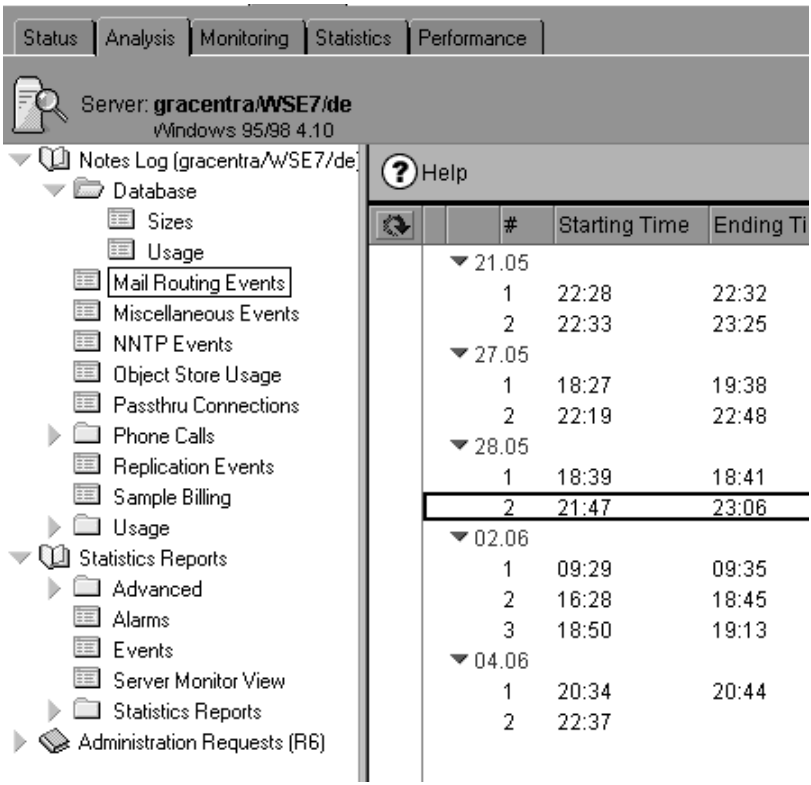
Der Reiter "Status" enthält eine Übersicht über die Hauptaufgaben, die ein Lotus Domino Server zu bewältigen hat. Dazu gehören:

- Hintergrund-Tasks, die vom Server ausgeführt werden, ohne dass ein Benutzer etwas dazu tun muss, nachdem sie einmal eingerichtet wurden
- Benutzer
- Datenbanken, die geöffnet wurden

Auch wenn es nur ein Überblick ist, erhält man hier sofort einen Eindruck, wie viele Benutzer gerade am System aktiv sind, mit was sie beschäftigt sind und welche Datenbanken von mehreren Benutzern aufgerufen wurden. Auch in der Task-Übersicht wird auf einem Blick klar, wie viele und vor allem auch welche Tasks laufen. Dies kann vor allem dann wichtig sein, wenn bei der Überwachung des Servers eine hohe Auslastung festgestellt wurde und der Administrator ad hoc sehen will, wer im System ist und was gerade passiert.

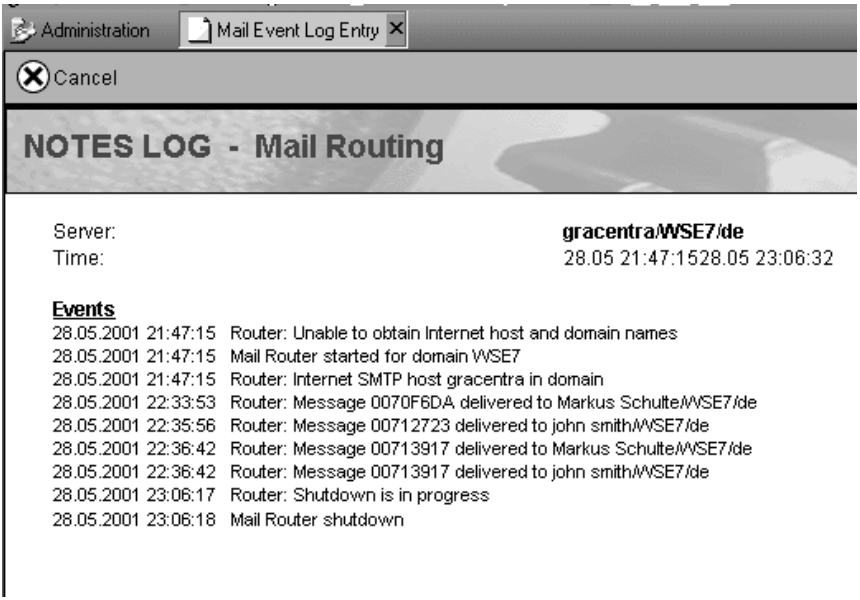
11.2.2.2 Analyse

Soll zu einem späteren Zeitpunkt kontrolliert werden, was wann passiert ist, dann fängt man am einfachsten bei diesem Register zu suchen an. Der Lotus Domino Server sammelt alle Daten, die für statistische Auswertungen und Analysen benötigt werden, automatisch. Hier werden die gesammelten Daten in den unterschiedlichsten Ansichten dargestellt: Mail, Weiterleitungsereignisse, Telefonanrufe, Replikationsereignisse usw.



Übersicht Analyse

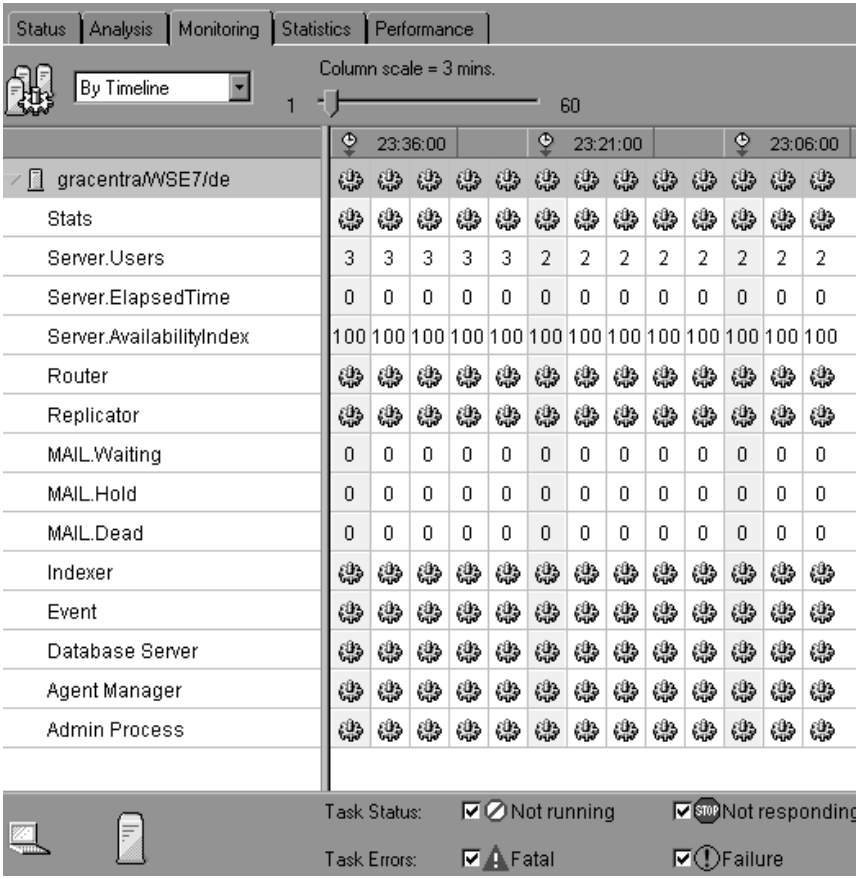
Mit einem einfachen Doppelklick sind die einzelnen Ereignisse im Detail zu sehen.



Analyse im Detail

11.2.2.3 Monitoring

Wie bereits erwähnt gibt es mehrere Möglichkeiten, den Lotus Domino Server auch direkt zu überwachen. Hinter dem Reiter "Monitoring" verbirgt sich eine dieser Möglichkeiten.

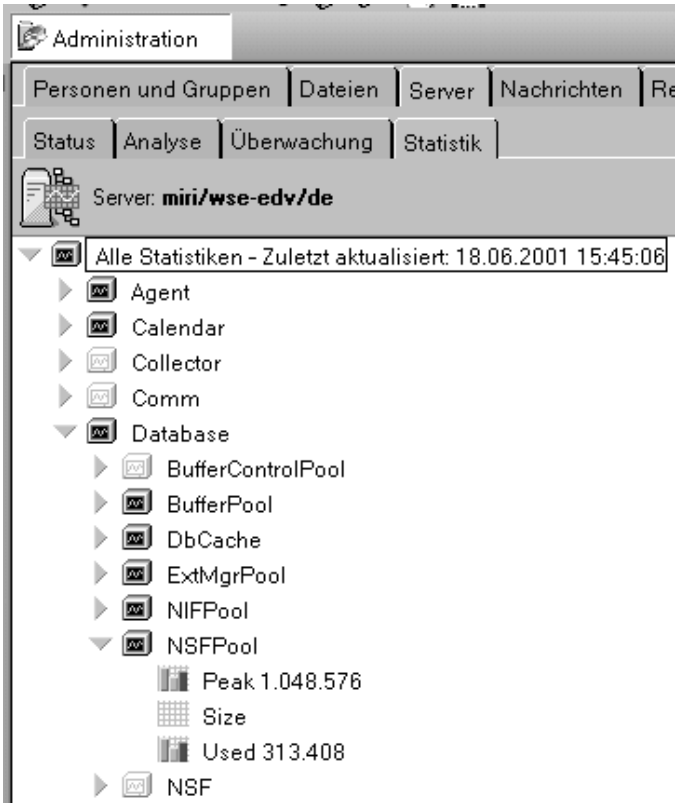


Monitoring

Hier werden wesentliche Kenngrößen (Anzahl der Benutzer, Server-Verfügbarkeit, wartende e-Mails und einige, wesentliche Server-Tasks und deren Verfügbarkeit) über die Zeit hin dargestellt. Entsprechend dem eingestellten Intervall (1-60 Minuten) werden sie vom Server neu angefordert und in der Übersicht aktualisiert. Je nach Anzahl der installierten Server können auch mehrere Server angezeigt und überwacht werden. Dabei ist der Standort der Server unerheblich. Lediglich die Übertragung der Daten für die Überwachung wirkt sich dabei aus.

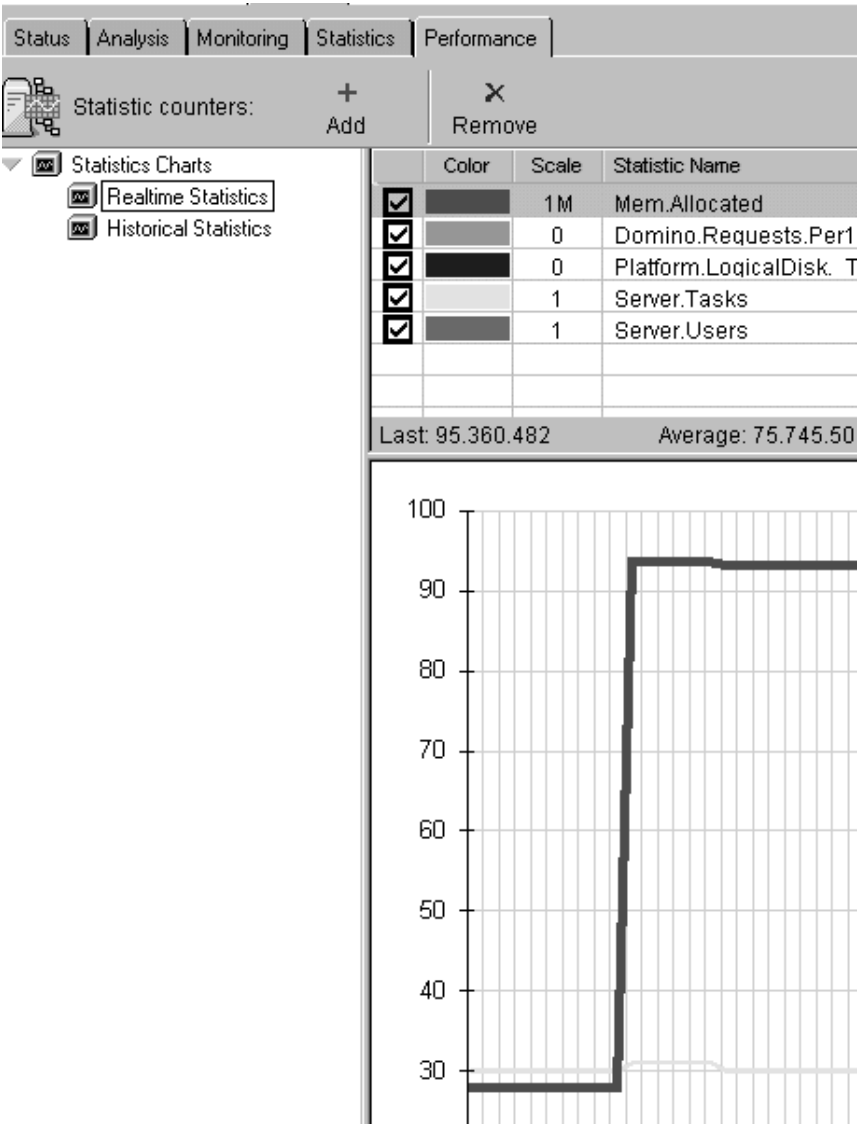
11.2.2.4 Statistik und Performance

Die beiden restlichen Kategorien gehören im Grunde zusammen. Nachdem man auf den Reiter "Statistik" geklickt hat, werden die verschiedenen Werte (ACL, Bufferpool, Database) mit deren Überbegriff (Database) aufgeklappt. Wenn zusätzliche Agenten wie z. B. DECS installiert wurden, dann werden deren Kontroll- und Steuerungswerte hier auch aufgenommen.



Statistik

Vorteilhaft an dieser Darstellung ist die Übersichtlichkeit: Zusammengehörige Kennzahlen sind auch unter einem Überbegriff gesammelt. Dass dabei immer nur der letzte ermittelte Wert zur Verfügung steht, wirkt sich dagegen schnell nachteilig aus. Um hier eine Alternative zu bieten, wurde der Bereich Performance geschaffen. Alle unter dem Reiter "Statistik" angebotenen Einzelwerte können hier im Zeitverlauf als Grafik dargestellt werden. Pro ausgewählter Kennzahl können die Werte in einer Übersicht ausgegeben werden. Zusätzlich sind in einer Statuszeile der letzte Wert, der Durchschnitt über den Zeitverlauf, das Minimum und das Maximum aller Werte und die Dauer der Untersuchung zu sehen. Die Kennzahlen können für mehrere Server zusammengefasst werden. Unterschiedliche Auswertungen können als Profil gespeichert werden.



Performance im Zeitablauf

Um sich ein Bild über den aktuellen Zustand des Lotus Domino Servers zu machen, kann man sich zunächst auf die folgenden Werte konzentrieren.

Prozessor

- Prozessorauslastung in Prozent: Werte kleiner als 80 Prozent sind zu bevorzugen.
- Prozessorwarteschlange: Anzahl der Anfragen, die darauf warten, abgearbeitet zu werden. Kleine Werte sind besser.

Hauptspeicher

- Seiten/Sekunde: Seiten, die von der Festplatte gelesen oder geschrieben werden, um Anfragen zu erfüllen, die sich nicht im Speicher befinden. Werte kleiner als 20 sind ausreichend.
- Geschriebene Bytes: Speicher einschließlich des Pagefile-Festplattenbereiches, die weggeschrieben wurden. Der Wert sollte nicht größer als 70 % des gesamten Hauptspeichers sein.

Festplatte

- % Disk Time: Die Zeit in Prozent, während der die Festplatte beschäftigt ist. Niedrige Werte sind besser, ein Wert > 70 % deutet auf einen Engpass in diesem Bereich hin.
- Durchschnittliche Zeit in Sek./Transfer: Je kleiner der Wert, desto schneller werden die Daten auf die Festplatte geschrieben. Kleine Werte sind zu bevorzugen.

Netzwerk

- Bytes Total/Sek.: Die Anzahl der Bytes, die insgesamt pro Sekunde auf dem ausgewählten Netzwerkadapter übertragen werden. Dauerhaft hohe Werte deuten auch hier wieder auf einen Engpass hin.

Lotus Notes Subsystem

- Server-Verfügbarkeitsindex: Dieser Wert gibt an, wie hoch die Auslastung des Servers zu einem bestimmten Zeitpunkt war. Große Werte sind besser.
- Server.Sessions.Dropped: Die Anzahl der Sitzungen, die vom Server aus beendet wurden. Dies geschieht, wenn am Client nichts getan wird. Kleine Werte sind zu bevorzugen.
- Server.User: Die Anzahl der verbundenen Benutzer ist interessant, um die Lastverteilung während des Tages zu untersuchen und automatische Tasks entsprechend antizyklisch starten zu lassen.

Neben dieser Auswahl bietet der Lotus Domino Server eine große Anzahl von weiteren Kennzahlen.

Hardware und Betriebssystem bilden die Grundvoraussetzungen für eine ausreichende Performance. Im nächsten Schritt hängt die Leistung des Systems entscheidend davon ab, wie seine Nutzung auf die verschiedenen Komponenten verteilt ist. Ein reines e-Mail-System (wie es die Hersteller bei ihren Performance-Messungen unterstellen) wird sich völlig anders verhalten, als ein System, in dem unterschiedliche Notes- und Domino-Anwendungen eingesetzt werden. Deshalb bietet Lotus mit dem Administrator-Client

Werkzeuge, die genauere Informationen über einzelne Leistungsbereiche liefern.

Wichtig sind für ein Unternehmen bei der Performance-Messung in diesem Zusammenhang zwei Dinge:

- **Aufbau einer Sammlung von Leistungsdaten**
  Für präzise Aussagen über die aktuelle und zukünftige Leistungsfähigkeit eines Lotus Domino Servers ist es wichtig, ständig Daten zu sammeln, damit Vergleichswerte existieren, wenn die Performance nicht mehr den Anforderungen entspricht. Nur dann ist schnell erkennbar, in welchem Bereich des Systems Handlungsbedarf besteht.

- **Grenzwerte festlegen**
  Als zweites können auf der Basis dieser Kennzahlen Grenzwerte festgelegt und mit Alarmmeldungen überwacht werden. Damit ist es oft möglich, Engpässe zu erkennen, bevor es zu spät ist und der Lotus Domino Server nicht mehr zur Verfügung steht.

Performance ist ein Thema seit es Computer-Systeme und Anwender gibt. Auch wenn die Hardware immer leistungsfähiger wird, so wird dieses Thema noch lange erhalten bleiben. Es ist gut, sich darauf einzustellen.

11.3 Diverse Datenaustauschtools

Oftmals werden für den Datenaustausch zwischen Domino und Nicht-Domino-Anwendungen die „Standardlösungen" DECS und LEI genannt. Sicher sind diese in komplexen Umgebungen auch meist die richtige Wahl, für kleine Anforderungen jedoch der berühmte „Schuss mit Kanonen auf Spatzen".

Lotus bietet neben diesen Tools auch eine Reihe von kleinen Werkzeugen, die als Freeware zur Verfügung stehen und die für die Realisierung einfacher Anforderungen im Bereich des Datenaustauschs mit „dem Rest der Welt" eingesetzt werden können – und dies ohne langes Studieren von Anleitungen oder komplexen Installationen. Diese Tools haben, obwohl es sie zum Teil schon seit mehreren Jahren gibt, einen geringen Bekanntheitsgrad. Grund genug also, sie wenigstens an dieser Stelle zu erwähnen – denn vielleicht lässt sich eine einfache Anforderung mit einem dieser Tools auch ohne Programmierung realisieren.

Diese Seite ist zur Zeit nicht belegt.

11.3.1 DB2 Client Import Library

Unter den verschiedenen Möglichkeiten des Datenaustauschs zwischen Domino und iSeries kann für kleinere Importe die „DB2 Client Import Library“ verwendet werden. Dabei handelt es sich um ein Freeware Tool der IBM, das Sie übers Internet herunterladen können und das, wie der Name schon sagt, die Möglichkeit bietet, iSeries-Informationen auf den Notes Client zu importieren. Es werden mit diesem Tool keine Export-Funktionen aus Notes heraus angeboten. Für viele „kleine“ Zugriffe auf DB2-Daten ist dieses schlanke Werkzeug aber eine praktische und leicht zu bedienende Integrationsmöglichkeit, die keine Programmierkenntnisse erfordert.

Ebenfalls im Namen bereits enthalten ist auch die zweite Einschränkung, nämlich der Einsatz nur in Verbindung mit DB2-Datenbanken als externe Datenquelle.

Wenn Sie aber recht schnell und ohne Aufbereitung auf in Notes integrierte Informationen der iSeries zugreifen wollen, dann könnte dieses Tool eine Alternative zu Programmierzugriffen oder zum Einsatz von DECS oder den kostenpflichtigen Tools sein.

Die Voraussetzungen sind ähnlich schlank wie das Produkt selbst:

11.3.1.1 Voraussetzungen

Für die Installation der DB2 Client Import Library benötigen Sie einen WIN-basierten Client. Das Tool ist bereits seit einigen Jahren verfügbar – deshalb auch die Unterstützung ab Win3.11 bis hin zu WinXP.

IBM bietet darüber hinaus auch noch eine OS/2-Variante an, die wohl nur die Wenigsten benötigen werden. Dasselbe gilt für die WIN16-bit-Version – die neben der 32-bit-Version zum Download bereitsteht.

Neben den Betriebssystemen Windows oder OS/2 ist eine ODBC-Verbindung zur iSeries zwingend erforderlich. Dabei ist es irrelevant, ob die ODBC-Funktionalitäten von iSeriesAccess (oder Client Access) verwendet werden oder ODBC-Produkte von Fremdanbietern.

Die DB2 Client Import Library basiert auf der Ausführung von SQL Stored Commands, deshalb sollte der Anwender wenigstens Grundkenntnisse im Umgang mit SQL haben.

Im Gegensatz zu anderen Integrationsprodukten ist die Menge der erforderlichen Voraussetzungen recht übersichtlich.

Eine kleine Einschränkung:
Der Import der Informationen ist auf RichText-Felder beschränkt. Für eine immer wiederkehrende Anforderung wie zum Beispiel „aktuelle Umsatzzahlen“ sollte dies aber wenig stören.

Schauen wir uns das Tool nun näher an.

11.3.1.2 Download

Zunächst kann es unter der Adresse www.iseries.ibm.com/domino/db2import.htm heruntergeladen werden. IBM verlangt zwar einen Benutzer und ein dazugehöriges Kennwort – aber keine Angst, es fallen keine Kosten an und wenn man den Klick an „keine

Werbemails“ setzt, werden die Daten auch nicht „missbraucht“. Der Download selbst umfasst zwei .dll-Dateien, eine .nsf-Datei und eine .QRY-Datei mit einem Beispiel für die Definition einer entsprechenden Abfrage.

Download-Dateien

DLL-Dateien kopieren

Nach dem Download müssen die Dateien entpackt werden. Dabei werden zunächst die beiden DLL-Dateien in das Notes-Programm-Verzeichnis kopiert. Achten Sie unbedingt darauf, dass die Dateien nicht in das „DATA“-Verzeichnis gestellt werden!

NSF-Datei kopieren

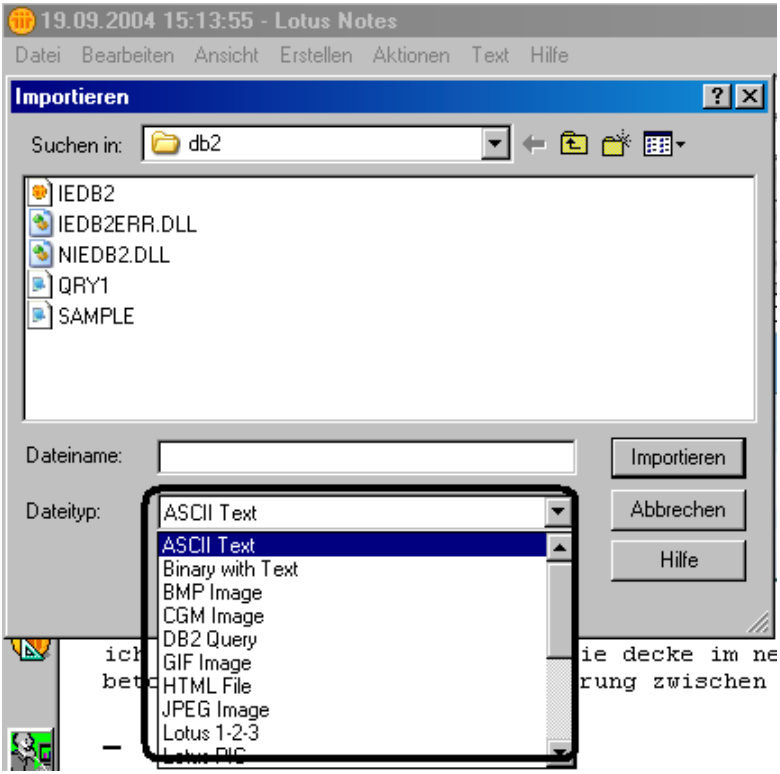
Die .NSF-Datei IEDB2.NSF wird in das „DATA“-Verzeichnis des Notes-Client kopiert. Hier unbedingt darauf achten, dass Sie das „DATA“-Verzeichnis verwenden!!

Anpassen der NOTES.INI

Damit die Import-Funktionen genutzt werden können, muss die NOTES.INI angepasst werden. Dabei wird eine weitere EDITIMP-Angabe erfasst. In der Regel befinden sich in der NOTES.INI bereits Einträge des Typs „EDITIMP" – denn mit diesen Einträgen wird festgelegt, welche Dateitypen bei der Auswahl „Datei / Import" zur Verfügung stehen.

```
EDITIMP16=WordPerfect 5.x,0,_IW4W,,.DOC,.WPD,,2,
EDITIMP17=WordPerfect 6.0/6.1,0,_IW4W,,.DOC,.WPD,.WPT,,2,
EDITIMP18=DB2 Query,0,_IEDB2,,.QRY,
EDITEXP1=ASCII Text,2,_XTEXT,,.C,.H,.PRN,.RIP,.TXT,,1,
EDITEXP2=CGM Image,2,_XCGM,,.CGM,.GMF,,8,
EDITEXP3=Microsoft RTF,2,_XRTF,,.DOC,.RTF,,4,
```

NOTES.INI

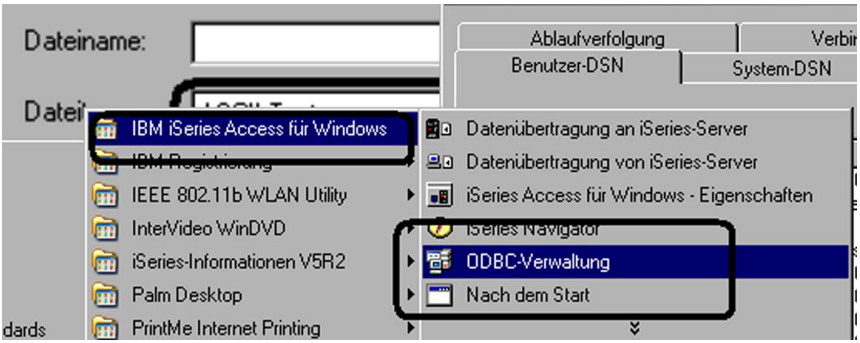


Import-Dateitypen

11.3.1.3 ODBC-Verbindung

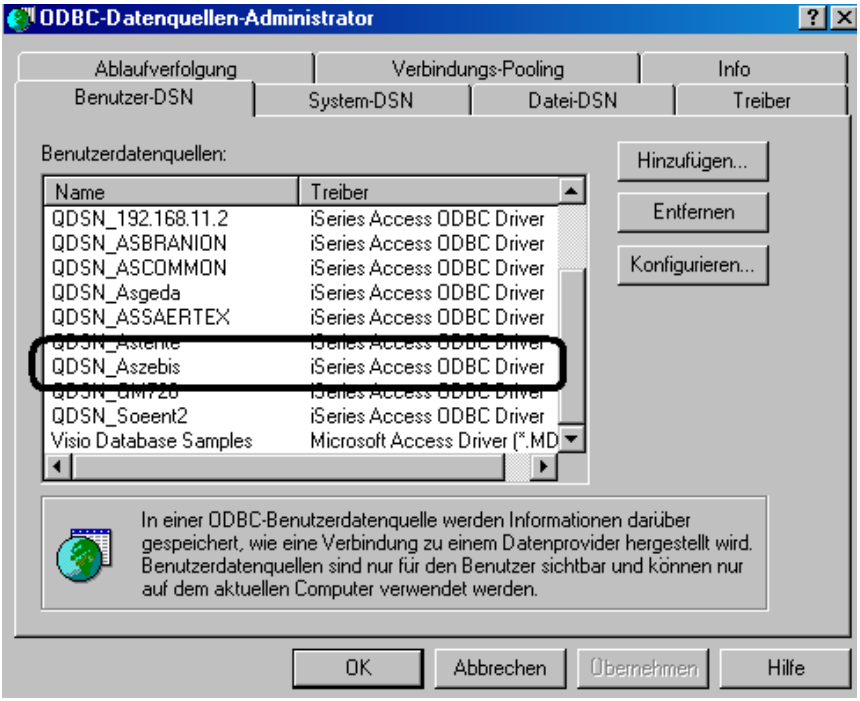
Die Basis für die Kommunikation zwischen Notes und der iSeries stellt eine ODBC-Verbindung dar. Häufig findet man im iSeries-Umfeld das Lizenzprogramm iSeriesAccess (das frühere Client Access). Einer der Bestandteile dieses Produkts ist ein ODBC-Produkt, das auch für den Einsatz des DB2-Import-Tools verwendet werden kann. Der Einsatz des DB2-Import-Tools ist aber nicht zwingend an den Einsatz der iSeriesAccess-ODBC-Komponente gebunden, sondern kann vielmehr mit jedem ODBC-Tool eingesetzt werden, das eine Verbindung zu einer iSeries ermöglicht. Im nachfolgenden Beispiel haben wir die iSeriesAccess-ODBC-Komponente verwendet.

Wichtig ist das Erstellen einer Verbindung zur iSeries. Dazu wählen wir zunächst in der Programmgruppe „iSeriesAccess" „ODBC-Verwaltung" aus.



ODBC-Verbindung

In der folgenden Anzeige befinden sich die konfigurierten ODBC-Verbindungen. Unter anderem auch die Verbindung zur iSeries. Sollte diese noch nicht vorhanden sein, so kann sie durch einen Klick auf die Schaltfläche „hinzufügen“ erstellt werden.



ODBC-Übersicht

11.3.1.4 ODBC-Definition in Notes

Damit Notes mit der ODBC-Schnittstelle kommunizieren kann, muss zunächst definiert werden, welche ODBC-Verbindung verwendet werden kann. Die Angaben dazu werden in der mit dem Tool zur Verfügung gestellten Notes-Datenbank „IEDB2.nsf“ vorgenommen.

Dazu öffnen wir nun diese Datenbank, die wir zuvor in das Notes-Data-Verzeichnis kopiert haben.

Verbindung definieren

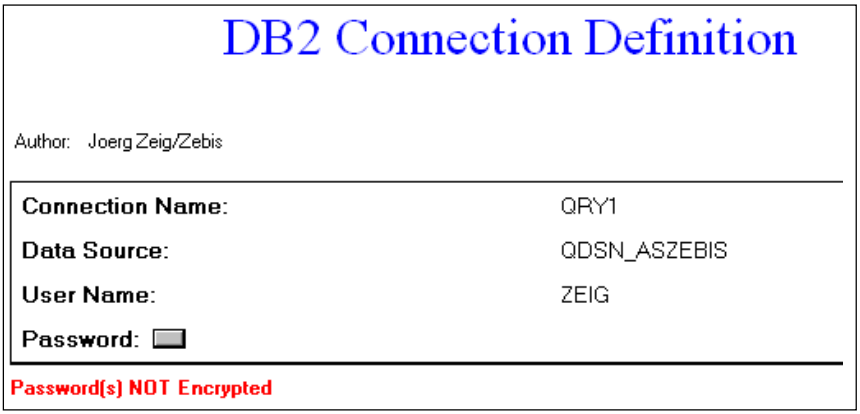
In der Datenbank sind nun die Definitionen für die Verbindung durchzuführen:

➢ Connection Name
- Dieser Name kann frei gewählt werden und beschreibt die Verbindung

➢ Data Source
- Dies ist der Name der ODBC-Verbindung. Er muss mit der Angabe in der ODBC- Definition übereinstimmen.

➢ Benutzername
- Hier muss der iSeries-Benutzer angegeben werden. Durch einen Klick auf die Schaltfläche neben dem Eintrag „Password“ kann die Verschlüsselung des Password initiiert werden.

All diese Angaben sind einmal pro Verbindung vorzunehmen.



Neue Verbindung

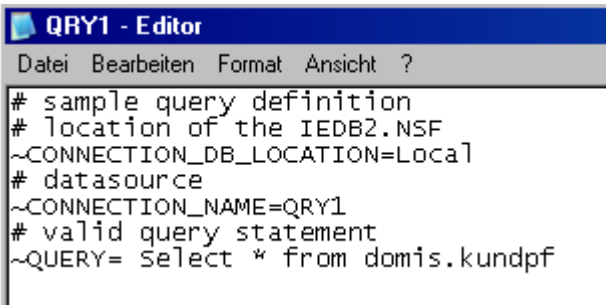
11.3.1.5 Erstellen einer .QRY-Datei

Für die Angabe der SQL-Statements dient auf dem Notes-Client eine .QRY-Datei. Diese beinhaltet unter anderem den Speicherort der Datei, den Server und die SQL-Anweisungen.

IBM liefert bereits eine Beispiel-„.QRY"-Datei mit, die einfach kopiert und für den eigenen Bedarf modifiziert eingesetzt werden kann. Der Name der Datei ist frei wählbar.

Wir haben in unserem Beispiel die Datei „QRY1.qry" genannt. Diese Datei kann in einem beliebigen Verzeichnis abgelegt werden.

QRY-Datei



Inhalt der QRY-Datei

Mit dieser Beispiel-QRY-Datei lesen wir auf der iSeries mit einer „SELECT“-Anweisung die Datensätze aus der Datei „domis.kundpf“ aus. Das Ergebnis wird dann in Notes importiert.
Die Parameter der Datei haben folgende Bedeutung:

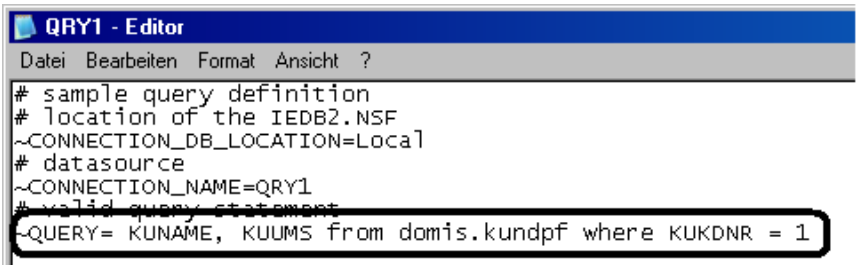
➢ „CONNECTION_DB_LOCATION“
- Speicherort der Notes-Datenbank
  – Z. B. “Local”

➢ „CONNECTION_NAME“
- Verbindungsname, der im Dokument der Datei „IEDB2.nsf“ angegeben wurde – in unserem Beispiel „QRY1“

➢ „QUERY“
- Angabe der SQL-Anweisungen

Alle Angaben, die mit einem „#“ beginnen, sind Kommentarzeilen, die in beliebiger Anzahl eingefügt werden können.

Je nach Anforderungen können die SQL-Anweisungen ebenfalls erweitert werden. Somit können zum Beispiel auch bedingte SELECT-Anweisungen angegeben werden.



Query Select mit Bedingungen

Nachdem wir nun die .QRY-Datei erstellt haben, können wir sie für den Import der gewünschten Informationen nutzen.

Voraussetzung ist der Import in ein Richtext-Feld.

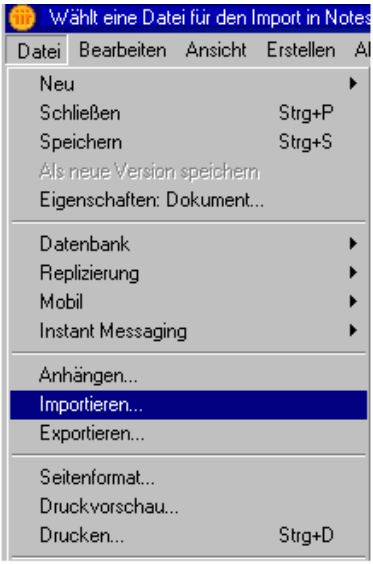
Nachfolgend nun der Import der Daten aus der DB2/UDB-Kundenstammdatei in ein Notes-RichText-Feld:

❶❷❸ Ausführungsschritte:

➢ Öffnen Sie in einer Notes-Datenbank – hier bietet sich eine „Kundenstammdatei“ an – eine Maske oder wählen Sie eine neue Maske zum Erstellen aus.

➢ Positionieren Sie den Cursor in einem Richtext-Feld

➢ Wählen Sie „Datei / Importieren“ aus

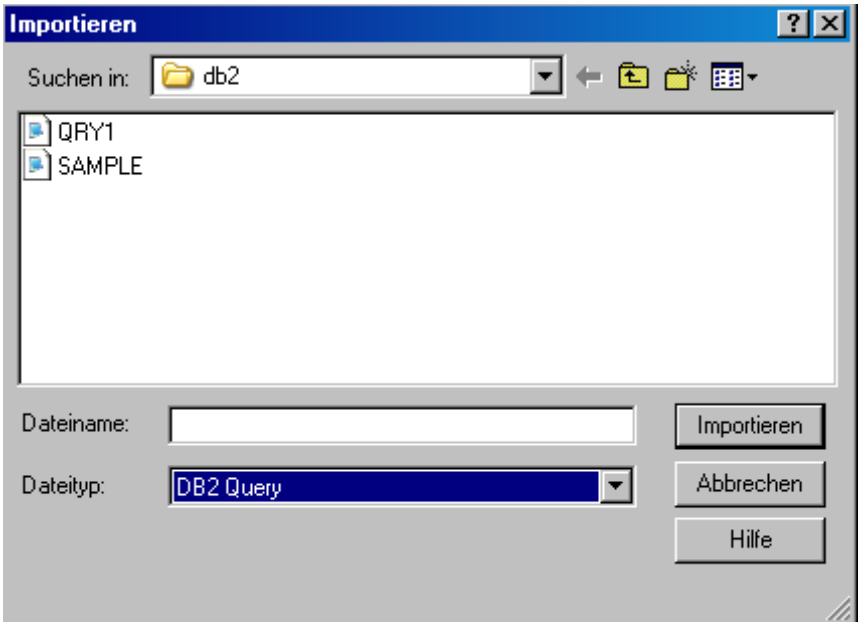


Import

➢ Wählen Sie im Import-Fenster zunächst den zu importierenden Dateityp unten in der Anzeige aus. Hier wird – durch das Hinzufügen der „EDITIMP“-Zeile in der NOTES.INI-Datei nun zu-

sätzlich der Eintrag „DB2 Query“ aufgelistet. Sollte dies nicht der Fall sein, prüfen Sie zunächst nochmals den Eintrag in der NOTES.INI. Ist er vorhanden, so sollte die NOTES.INI neu geladen werden – dazu beenden und starten wir Notes einfach.

Wenn Sie den Dateityp ausgewählt haben, geben Sie anschließend den Speicherort der .QRY-Datei an. In unserem Beispiel ist dies das Verzeichnis „DB2“ und die Datei heißt „QRY1.qry“.



Import-Angaben

➢ Nachdem Sie die Auswahl QRY-Datei getroffen haben, klikken Sie auf die Schaltfläche “Importieren”

Nun wird über die ODBC-Schnittstelle eine Verbindung zum angegebenen System aufgebaut und die in der QRY-Datei enthaltenen SQL-Anweisungen werden ausgeführt. Sollten diese fehlerhaft sein, so wird eine entsprechende Fehlermeldung ausgegeben. Im Erfolgsfall werden die Informationen aus der DB2/UDB ermittelt und in das RichText-Feld gestellt.

Das Ergebnis kann dann wie folgt aussehen:

Kundenstamm Demo Import DB2

Kundenstamm

KUKDNR	KUNAME	KUPLZ	KUORT
1	Willi Winzig	60000	Frankfurt
2	ITP Verlag	80000	Kaufering

Importergebnis

Zusammenfassung

Wie Sie in dieser kurzen Einführung gesehen haben, handelt es sich bei der „DB2 Client Import Library“ um ein schlankes Tool für den Import von DB2-Daten.

Vorteile:

➢ Schnelle Implementierung

➢ Kein Programmieraufwand

➢ Schneller Datenzugriff

➢ kostenlos

Nachteile:

➢ Nur Import möglich

➢ Nur Zugriff auf DB2/UDB möglich

➢ Beschränkt auf Verwendung in RichText-Feldern

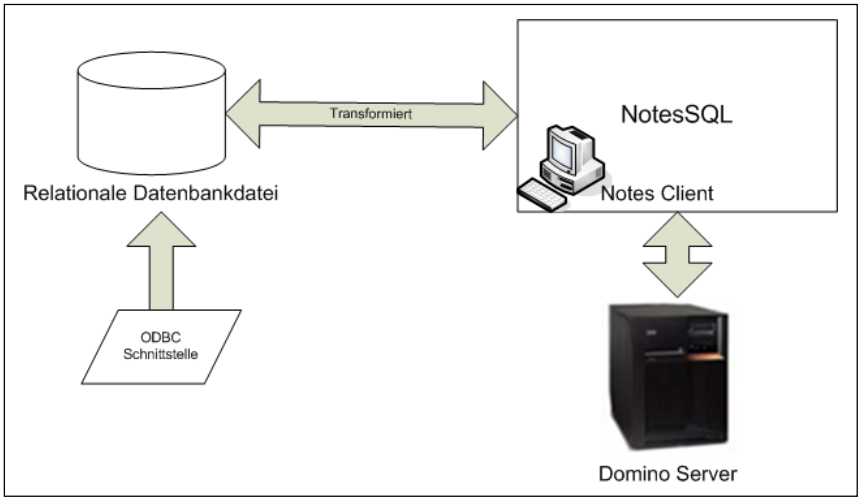
Diese Seite ist zur Zeit nicht belegt.

11.3.2 NotesSQL

Neben der zuvor gezeigten DB2 Client Import Library steht mit NotesSQL ein Toolset für den Notes Client zur Verfügung, das ebenfalls auf einer ODBC-Verbindung aufsetzt und über vorgefertigte Werkzeuge den Zugriff von Nicht-Domino-Anwendungen auf Domino-Daten ermöglicht. Dabei können die Daten wahlweise nur eingelesen, verarbeitet, verändert oder auch gelöscht werden.

Wie bei einigen anderen Werkzeugen auch, so besteht die Basis für den Einsatz dieses Tools in der Verwendung einer ODBC-Schnittstelle und entsprechenden SQL-Anweisungen.

Hintergrund für die Entwicklung von NotesSQL ist die Art und Weise, wie Informationen in Notes/Domino gespeichert werden, und wie andere Systeme darauf zugreifen können.



SQL-Einbindung

Im Gegensatz zu den Daten z. B. auf einer iSeries, wo wir von einer relationalen Datenhaltung sprechen, sind die Daten in Domino unstrukturiert gespeichert.

Diese Tatsache erschwert einen externen Zugriff auf Domino-Informationen. Mit NotesSQL kann eine Domino-Datenbank quasi „künstlich“ in das Format einer relationalen Datenbank umgesetzt werden, womit dann der Zugriff von exteren Anwendungen wesentlich vereinfacht wird.

Betrachten wir nun einmal den Aufbau von Notes-Daten. Die Stärken von Notes liegen in der Speicherung und Verarbeitung von unstrukturierten Daten und Informationen.

Jeder Datensatz in Notes kann aus einer beliebigen Anzahl unterschiedlicher Felder bestehen, deren Typ und Inhalt ebenfalls unterschiedlicher Art sein kann. In Notes sprechen wir bekannterweise auch von Dokumenten – den „Sammlungen“ einzelner Datenfelder.

Grundsätzlich werden alle Standarddatentypen in Notes als Listen oder Arrays abgespeichert.

Betrachten wir nun den Aufbau einer relationalen Datenbank wie zum Beispiel die DB2/UDB unserer iSeries:

Daten können hier in bestimmten vorgegebenen Bereichen und Typen abgespeichert werden.

Einige Entwickler sprechen bei den Speicher-Containern von „Tabellen“, andere von „Physischen Dateien“.

In diesen sind die Felder nach Typ und Länge fest vorgegeben.

Man kann sich nun vorstellen, dass die Verbindung von relativ „unstrukturierten“ Daten wie sie Notes liefert, mit solchen streng vorgegebenen Richtlinien, wie sie eine relationale Datenbank erwartet, recht schwierig werden kann.

Hier greift NotesSQL ein – das in der Lage ist, die Informationen entsprechend anzupassen bzw. umzusetzen.

Systemvoraussetzungen

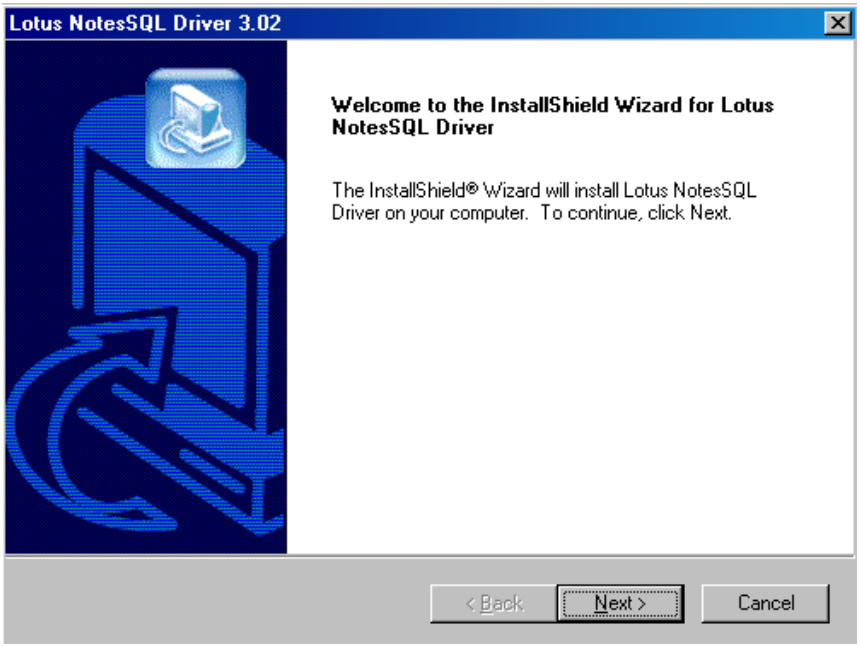
Für den Einsatz von NotesSQL müssen folgende Voraussetzungen erfüllt sein:

- WIN95, WIN98, WIN2000, WINXP, WINNT (mind. Service Pack 4)
- ODBC-Verbindung
- ODBC-Manager (mind. Version 3.0)
- Lotus Notes Client ab R5.0 oder
- Lotus Domino ab R5.0 oder
- Domino Designer ab R5.0

11.3.2.1 Installation

IBM bietet dieses Tool zum freien Download übers Internet unter der folgenden Adresse an: www.iseries.ibm.com/domino. Alternativ stellt die „Sandbox“ eine weitere Quelle für den Download dar.

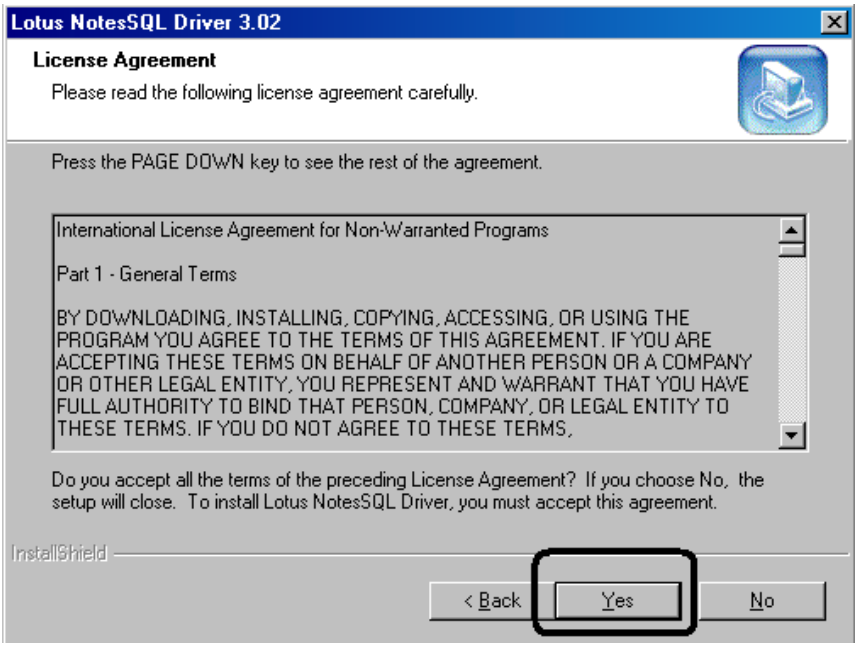
Nachdem Sie NotesSQL auf Ihren Rechner geladen haben, können Sie die .exe-Datei für die Installation aufrufen.



Installationsbeginn

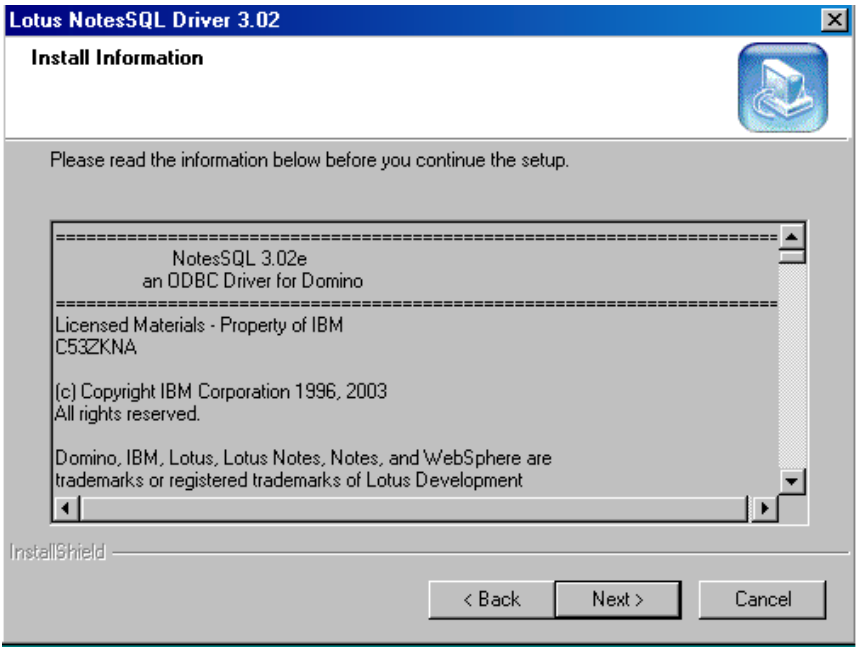
Die Installation läuft vergleichbar mit denen anderer Programme unter Windows ab. Klicken Sie in diesem Fenster auf die Schaltfläche „Next“.

Es erscheint das obligatorische Fenster mit den Lizenzbestimmungen, die Sie akzeptieren müssen, bevor mit der Installation fortgefahren werden kann.



Lizenzbestimmungen

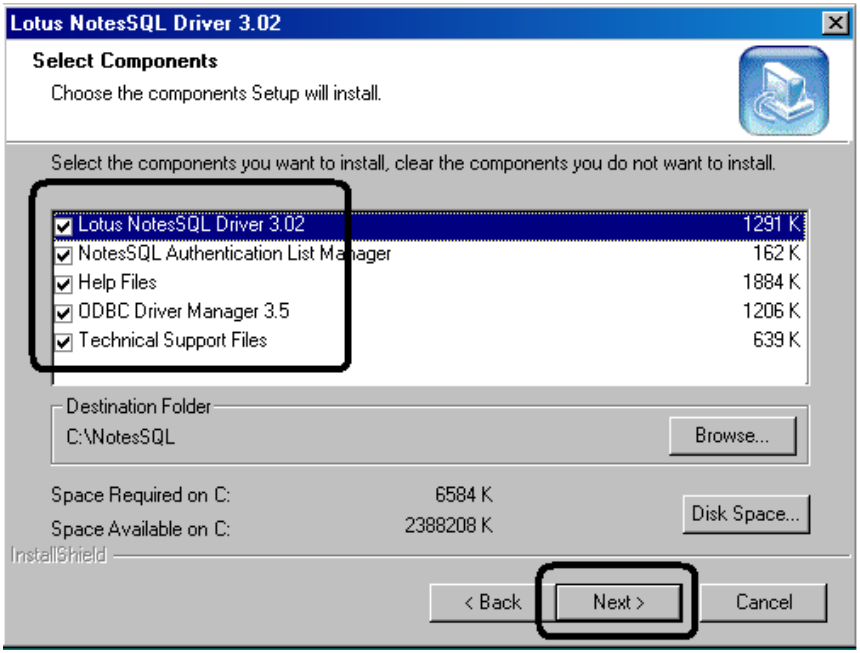
In der nächsten Anzeige erhalten wir einige Informationen über die zu installierende Software. Wichtig ist hier die korrekte Version.



Installationsinformationen

Ein erneuter Klick auf „Next“ setzt die Installation fort.

NotesSQL besteht aus einigen optionalen Teilbereichen, die in der nächsten Anzeige ausgewählt werden können. Spricht kein Grund dagegen, so empfiehlt sich die Installation aller Komponenten.



Komponenten installieren

Nach einem weiterer Klick auf „Next“ wird die Installation abgeschlossen und NotesSQL steht nun zur Konfiguration und für den späteren Einsatz bereit.

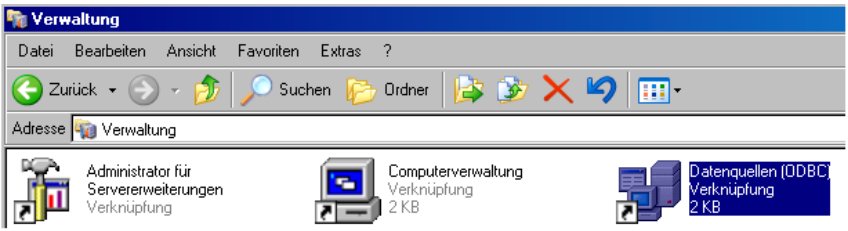
Für den Zugriff auf Daten mittels NotesSQL ist eine entsprechende ODBC-Verbindung erforderlich, die mit jedem verfügbaren ODBC-Treiber-Manager (ab Version 3) erstellt werden kann.

Im folgenden Beispiel verwenden wir den ODBC-Treiber von WinXP. Diesen finden wir unter

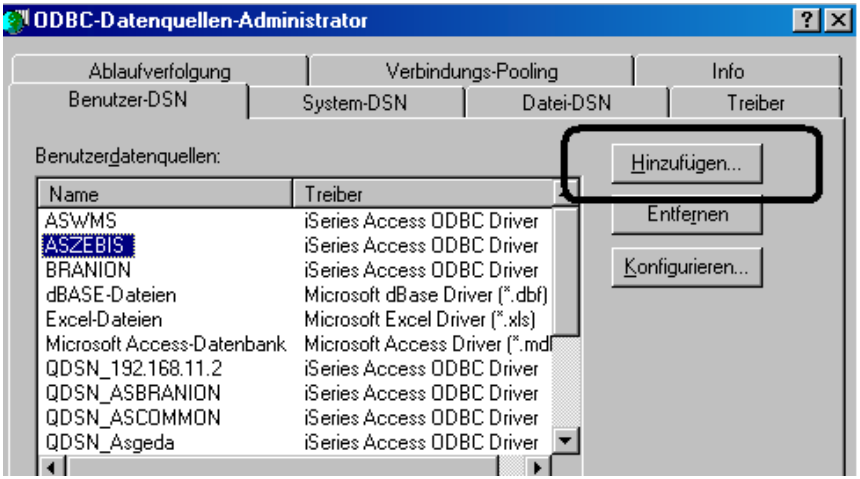
„Start / Einstellungen / Systemsteuerung“

➢ Wählen Sie nun „Verwaltung“ aus

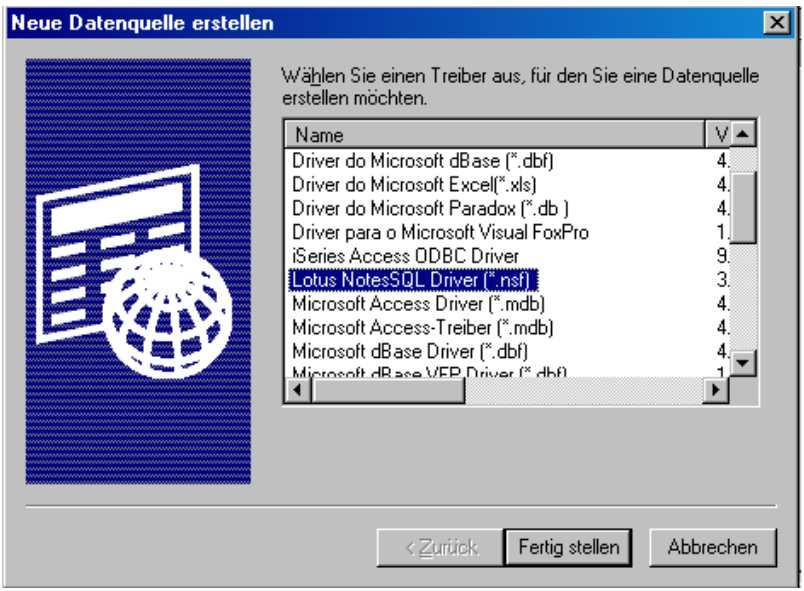
➢ Im Fenster „Verwaltung“ selektieren wir den Eintrag „Datenquellen ODBC“



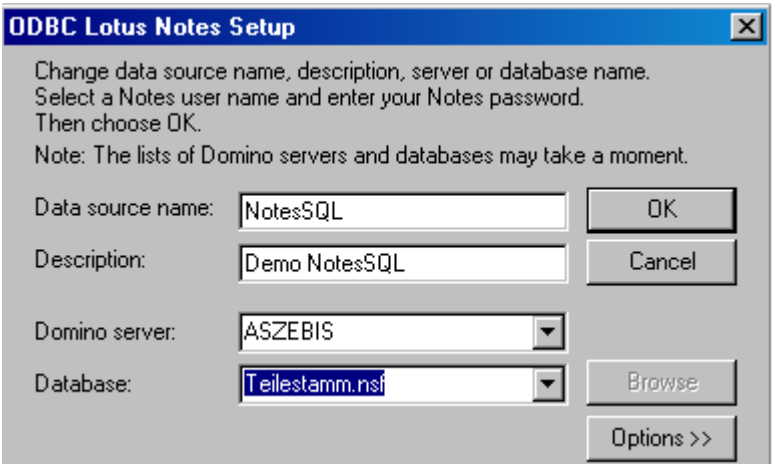
ODBC-Datenquelle



Hinzufügen



Datenquelle auswählen



Notes-Angaben

Als Data-Source-Name sollte ein möglichst sprechender Name verwendet werden. Dasselbe gilt für die Beschreibung.

Achten Sie darauf, dass der Notes-Benutzer, mit dem Sie sich angemeldet haben, auch über die erforderlichen Zugriffsrechte auf dem in dieser Abbildung auszuwählenden Domino Server verfügt, denn andernfalls wird in der Auflistung der auf dem Domino Server befindlichen Datenbanken keine Datenbank erscheinen.

In unserem Beispiel haben wir den Domino Server „ASZEBIS“ ausgewählt und im Feld „Database“ die Notes-Datei „Teilestamm.nsf“ selektiert. Durch einen Klick auf den Erweiterungspfeil können Sie eine Liste aller auf dem Domino Server befindlichen Dateien anzeigen und dort dann die gewünschte Datenbank selektieren.

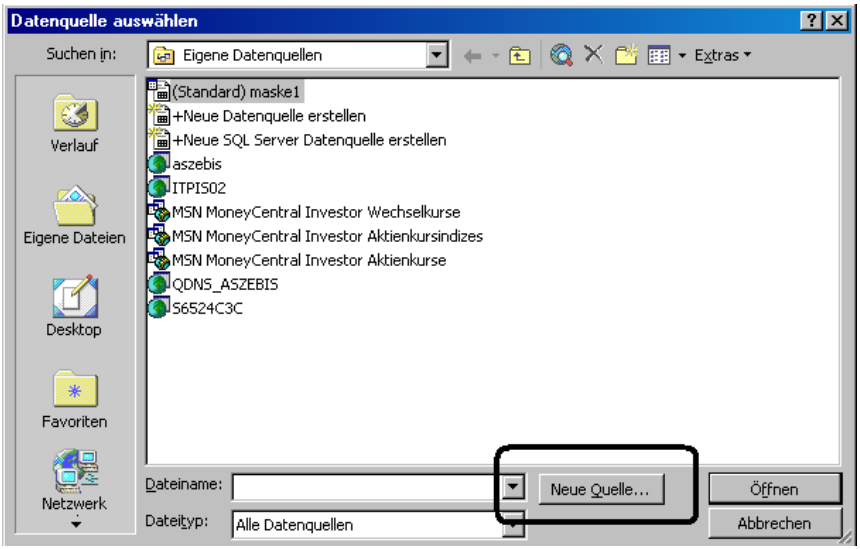
Diese neue Form der ODBC-Schnittstelle kann nun von allen möglichen Anwendungen genutzt werden.

Nehmen wir ein klassisches Beispiel: Microsoft Excel:

Hier kann über die „Import"-Funktion auf externe Daten zugegriffen werden. Leider ist der Zugriff auf Notes/Domino-Daten aus den zuvor erläuterten Gründen nicht möglich gewesen.

Schauen wir uns nun den Import mittels NotesSQL an:

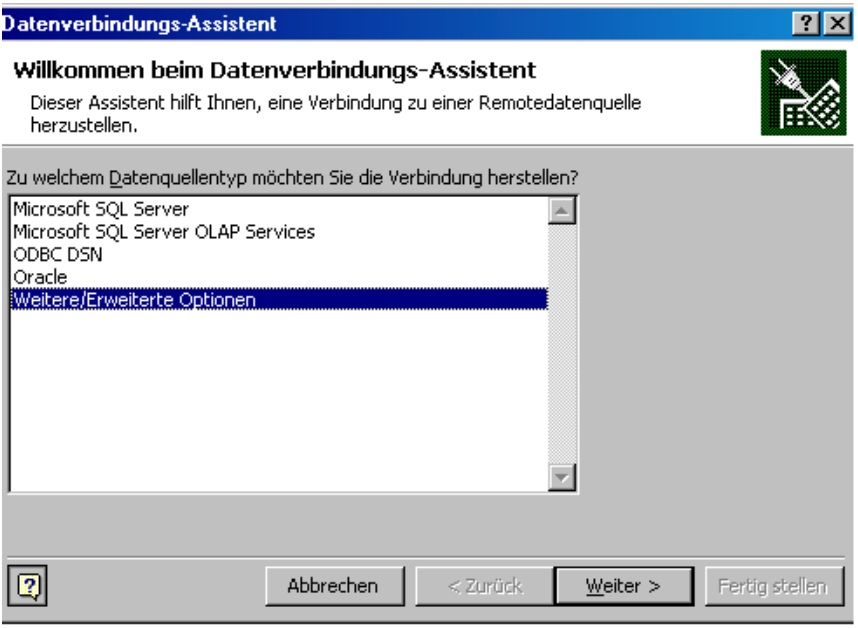
Dazu starten wir Excel und wählen in der oberen Fensterleiste „Daten / externe Daten importieren" aus.



Importangaben Excel

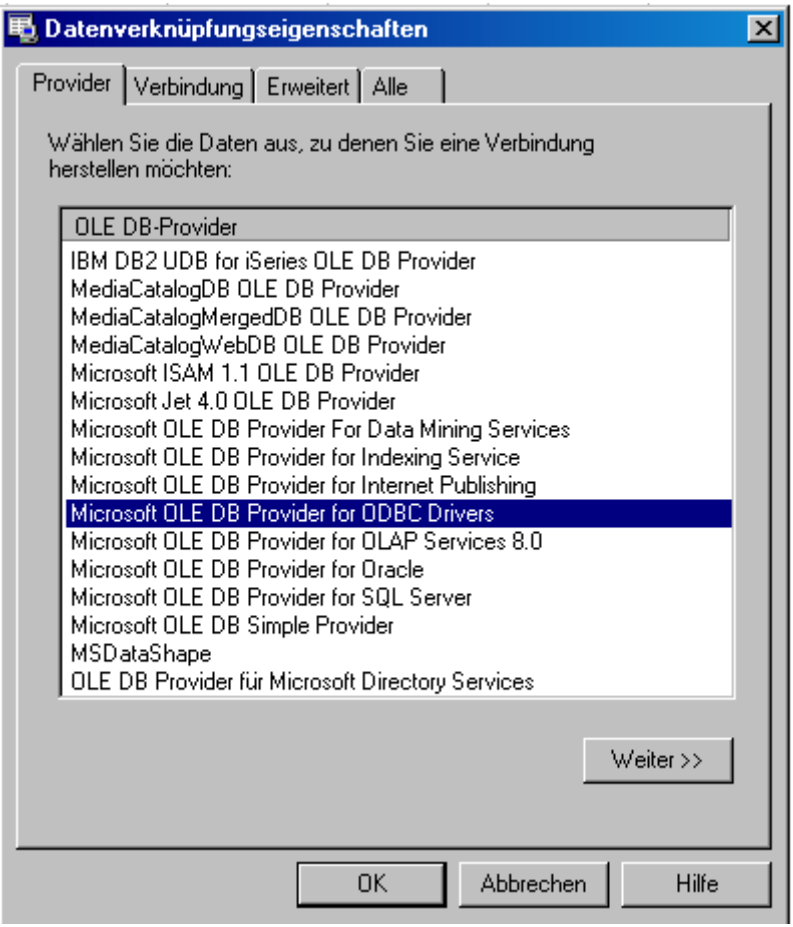
In diesem Fenster wählen wir den Abschnitt „Neue Quelle“ aus.

Nun wird der Datenverbindungsassistent gestartet. Hier wählen wir den Eintrag „weitere Optionen“ aus und klicken auf „Weiter“.



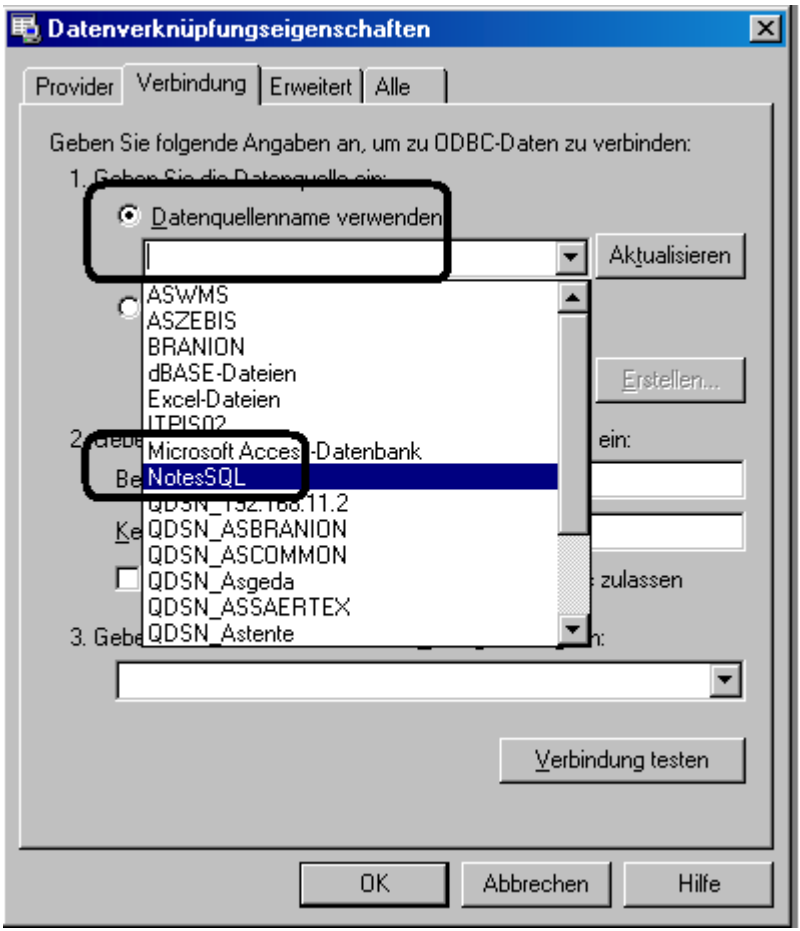
Datenverbindungsassistent

In der nächsten Anzeige ist bereits die Einstellung „OLE ODBC-Treiber“ voreingestellt. Wir akzeptieren diese Einstellung und klicken wieder auf „Weiter“.



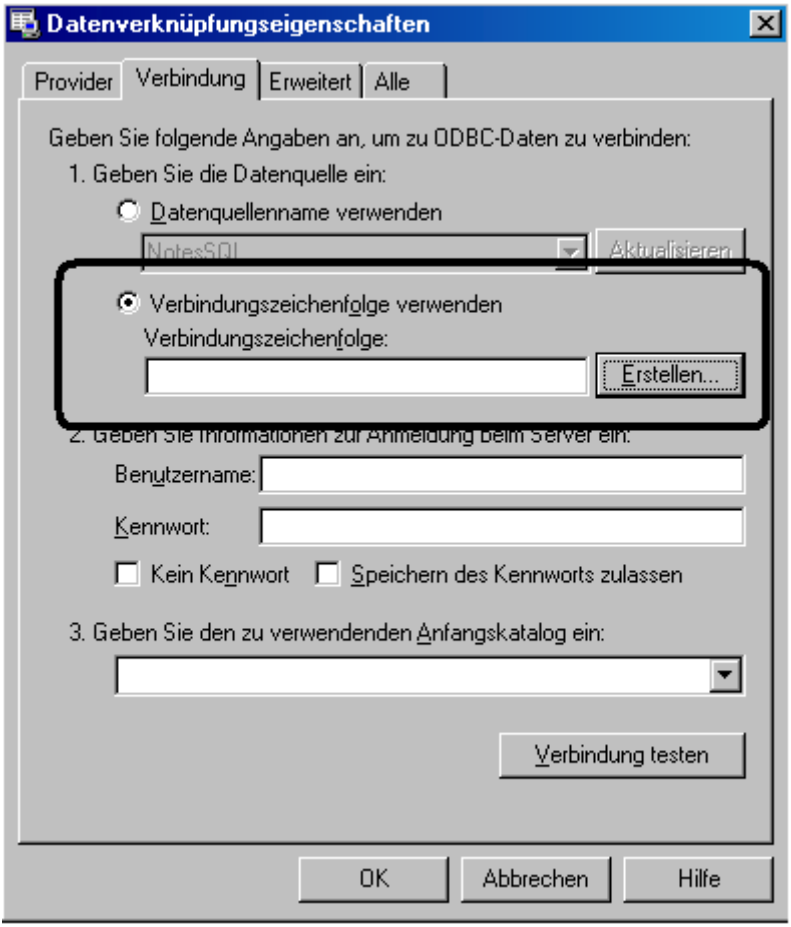
Datenverknüpfungseigenschaften

Im nächsten Fenster müssen wir einen Verbindungsnamen angeben. Klicken Sie auf „Aktualisieren“, dann erscheint ein Auswahlfenster, in dem u. a. auch der Eintrag „NotesSQL“ zu finden ist, den wir selektieren.



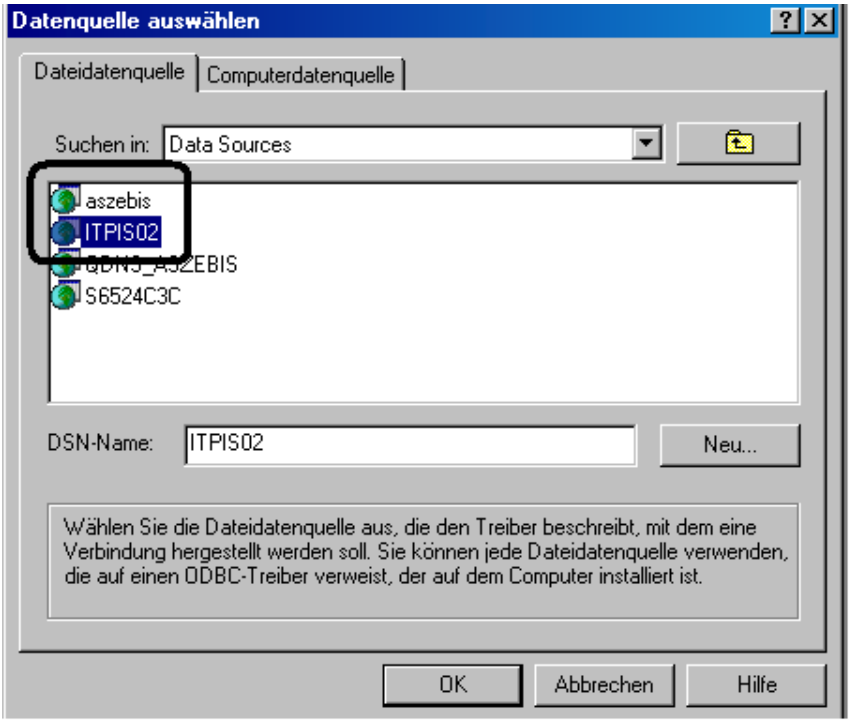
Datenquellname

Nach der Angabe des ODBC-Treibers definieren wir nun die so genannte Verbindungszeichenfolge. Dazu klicken wir auf die Schaltfläche „Erstellen“.



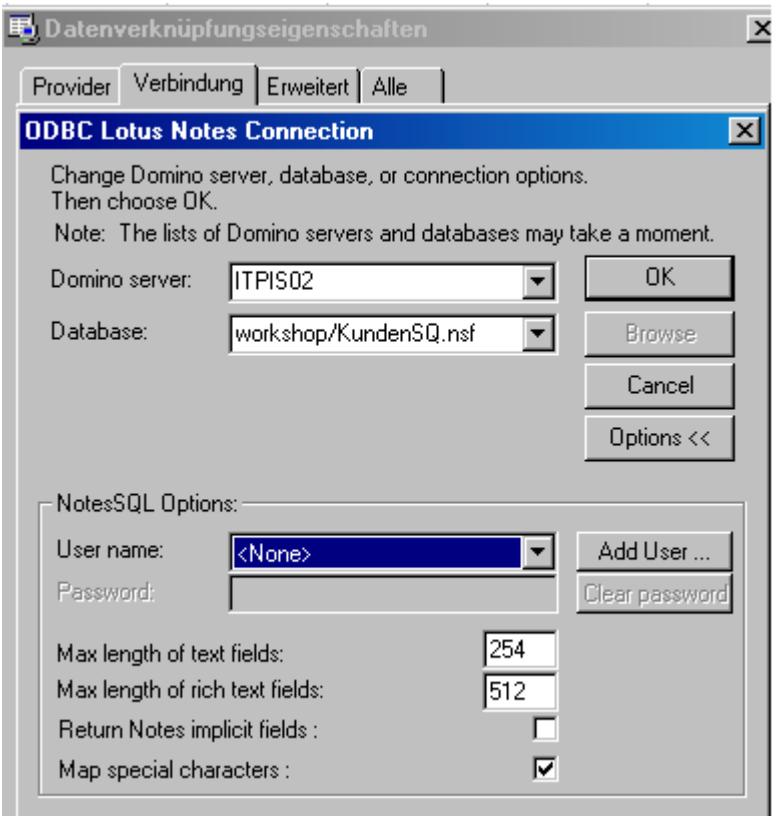
Verknüpfungseigenschaften

Als nächstes ist nun die Datenquelle anzugeben. In unserem Beispiel verwenden wir den Eintrag „ITPIS02“. Nachdem dieser ausgewählt ist, klicken wir auf „OK“.



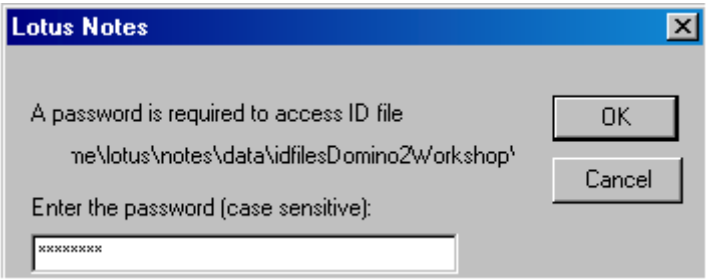
Datenquelle auswählen

Nun wird ein Fenster geöffnet, in dem u. a. die Datenquelle – also die Notes-Datenbank – ausgewählt werden kann. Zusätzlich kann ein Benutzername eingegeben werden. Wir lassen diesen in unserem Beispiel leer bzw. geben <NONE> an.



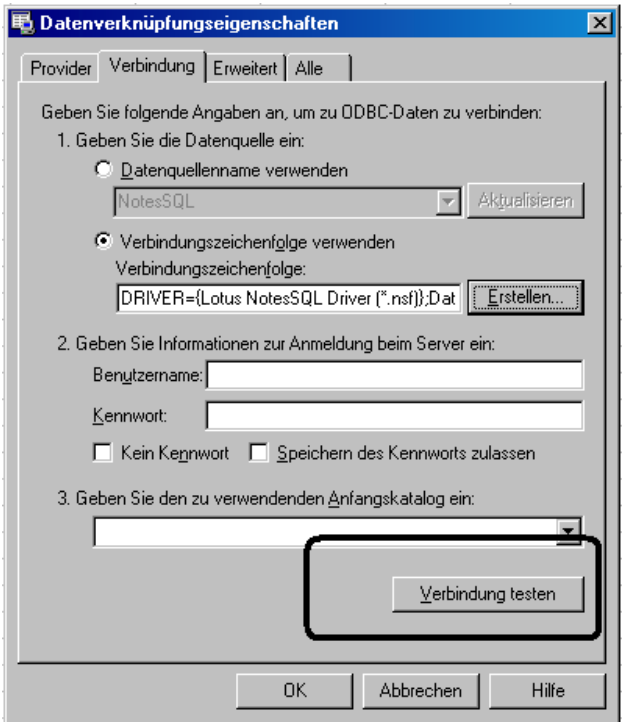
ODBC Connection

Damit eine Verbindung aufgebaut werden kann, müssen wir uns identifizieren:



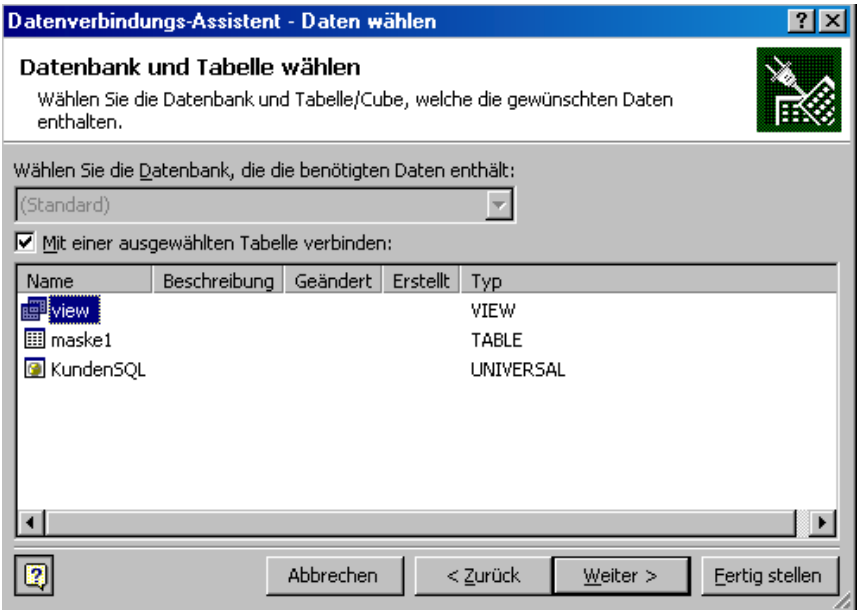
Login

Nun sollte unsere Definition der externen Datenquelle weitgehend abgeschlossen sein. In der nächsten Anzeige können wir die Verbindung testen. Ein Test sollte in jedem Fall erfolgreich sein!



Verbindung testen

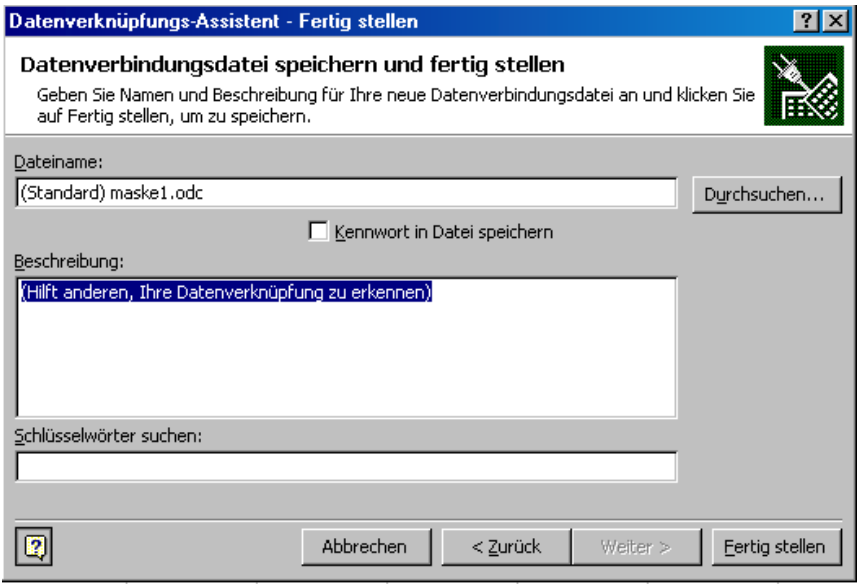
Nachdem wir auf „OK“ geklickt haben, können wir zwischen verschiedenen Elementen auswählen – dies sollte Ihnen aus Notes bekannt vorkommen:



Verbindungs-Assistent

In dieser Ansicht sind die Gestaltungselemente der Notes-Datenbank enthalten.

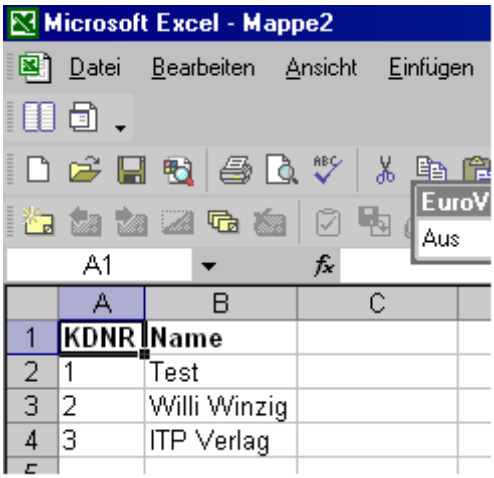
Wie wählen z. B. den Eintrag „maske1“ aus und klicken auf „Fertig stellen“.



Maske auswählen

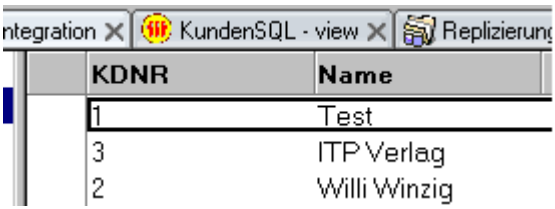
Nun sollte sich in Excel etwas „tun“:

Die Inhalte der in der Notes-Datei enthaltenen Dokumente werden in Excel importiert. Das Ergebnis kann so aussehen:



Excel Ergebnis

Die Notes Daten sahen/sehen so aus:



Notes-Daten

Diese Seite ist zur Zeit nicht belegt.

11.3.3 @Befehle

Für den Zugriff auf externe Dateien stehen auch in diesem Bereich einige (wenige) Befehle zur Verfügung, mit denen Daten externer Systeme verarbeitet werden können.

Basis hierfür ist ebenfalls eine ODBC-Verbindung, wie Sie weiter oben beschrieben ist.

Mit @Db-Befehlen lassen sich einzelne Werte oder ganze Listen aus einer relationalen Datenbank über ODBC einlesen und unter Verwendung des Befehls „@DBCommand“ auch wieder zurückschreiben.

Die Besonderheit bei der Verwendung der @DBCommand-Funktionen ist, dass sie nur in Verbindung mit SELECT-Anweisungen funktionieren.

Die @DB-Befehle im Überblick:

➢ @DBLookup
- Rückgabewert: Alle Werte, die dem definierten Schlüssel in der angegebenen Schlüsselspalte entsprechen.
- Vergleichbar mit einer SQL-Anweisung

„SELECT ….FROM….WHERE“

➢ @DBColumn
- Rückgabewert: Alle Wert einer Spalte
- Vergleichbar mit einer SQL-Anweisung „SELECT ….FROM“

➢ @DBCommand
- Rückgabewert: Alle Werte, die im Befehls-Statement angegeben sind.
- Verwendung aller SQL-Anweisungen

Achtung!

Für die Verwendung von @DB-Befehlen für den Zugriff auf externe Daten muss ein Eintrag in der NOTES.INI vorhanden sein, der diese Transaktionen steuert bzw. erlaubt.

Prüfen Sie deshalb die NOTES.INI auf diesen Eintrag:

```
NoExternalApps=1
```

Ist der Eintrag vorhanden, so ist die Ausführung der @DB-Befehle für einen Zugriff auf externe Daten deaktiviert. Wollen Sie dies ändern, so deaktivieren Sie diesen Eintrag in der NOTES.INI oder ändern Sie den Wert auf „0“.

11.3.3.1 @DBLookup

@DBLookup kann dazu verwendet werden, um mit einem Schlüssel auf Informationen eines externen Systems zuzugreifen, die diesem Schlüssel entsprechen.

Auf der iSeries könnte man als Vergleich den RPG-Befehl „CHAIN" heranziehen, mit dem ebenfalls über einen Schlüssel gezielt auf die Informationen einer Datei zugegriffen wird.

Aus SQL-Sicht würde dieser Befehl einem

„SELECT …FROM….WHERE"

entsprechen.

@DBLookup setzt auf den Angaben einer ODBC-Verbindung auf, über die der Datenaustausch realisiert wird. Der ODBC-Treiber setzt dabei dann die erforderlichen Aktionen ab, über die mit einem Schlüssel, der entweder eine Konstante oder ein Notes-Feldinhalt sein kann, auf eine externe Datei zugegriffen wird, über deren Schlüssel dann gezielt die Informationen eingelesen werden. Als Rückgabe kann dann der Wert eines Feldes der externen Datei verarbeitet werden. Mit @DBLookup können nur Lesezugriffe durchgeführt werden. Datenmanipulationen an den externen Daten sind somit nicht möglich!

Die Syntax für diesen Befehl muss wie folgt angegeben werden:

@DBLookup(„ODBC":"NoCache";
„externeVerbindung";"BenutzerID1:BenutzerID2“;
„Kennwort1:Kennwort2"; „externeDatei"; „Rückgabewert";
„Schlüssel externe Datei"; SchlüsselNotes";Distinct").

Schauen wir uns das an einem kleinen Beispiel an:

Die Datei auf der iSeries befindet sich in der Bibliothek „DOMIS“ und heißt „KUNDPF1“. Diese Datei enthält die folgenden Informationen:

```
Satzformatname:        KUNDR        EMPLOYEE MASTER
  1 KUNDENNR                             A       6        1   6 KUKDNR
  2 KUNDENNAME                           A      30        7  36 KUNAME
  3 POSTLEITZAHL                         P       7  0     37  40 KUPLZ
  4 ORT                                  A      30       41  70 KUORT
  5 UMSATZ                               P       9  2     71  75 KUUMS
  6 VERTRETER                            A      10       76  85 KUVERT
  7 KUNDENART                            A      10       86  95 KUART
```

Dateiaufbau

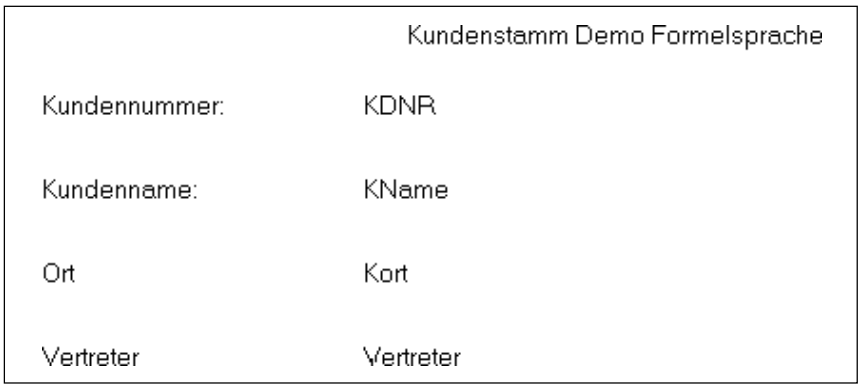
Der Inhalt dieser Datei:

KUNDENNR	KUNDENNAME
A	Test1
2	Meier

Datensätze

In Notes haben wir einen Kundenstamm, in dem wir nach Eingabe der Kundennummer den Kundennamen automatisch aus dem DB2-Kundenstamm übernehmen wollen.

Die Maske „Kundenstamm“ sieht in Notes so aus:



Maske Kundenstamm

Das Feld „KName“ soll in diesem Beispiel berechnet werden. Dazu wird der Wert des Feldes „KDNR“ als Zugriffsschlüssel verwendet.

DBLookup

In der Literatur findet man eine Vielzahl von unterschiedlichen Anweisungsaufbauten – insbesondere die Verwendung der „“-Zeichen.

Die Syntax des oben angegeben @DBLookup schauen wir uns ein wenig genauer an. Achten Sie auch darauf, dass die Syntax bei einem ODBC-Zugriff ein wenig abweichend von einem „normalen“ DBLookup ist, der auf lokale Notes-Daten zugreift!

➢ „ODBC“
- dies ist eine Konstante die definiert, dass über eine ODBC-Schnittstelle eine Verbindung aufgebaut werden soll

➢ „cache“
- wahlweise kann auch „noCache“ angegegeben werden

➢ „S6524C3C“
- Name der ODBC-Verbindung – diese sollte mit dem Eintrag in WRKDRBDIRE übereinstimmen

➢ Benutzer / Kennwort
- An Stelle der „“-Zeichen können die Benutzer-ID und das Kennwort eingegeben werden

➢ „DOMIS.KUNDPF1“
- dies ist die Pfadangabe in Form von Bibliothek.Datei also die Bibl. Ist in diesem Beispiel die „DOMIS“ und die Datei heißt „KUNDPF1“

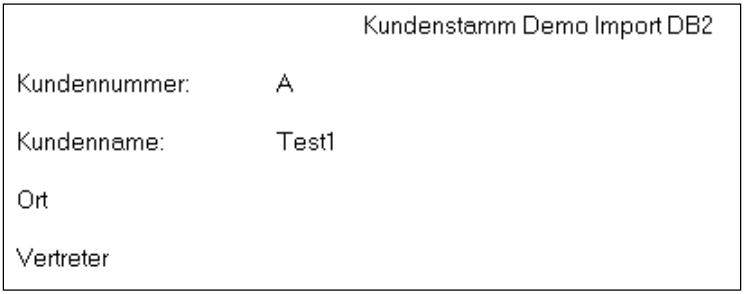
➢ „KUNAME“
- bei diesem Eintrag handelt es sich um den Namen des Feldes, das in Notes übertragen werden soll

➢ „KUKDNR“
- bei diesem Eintrag handelt es sich um den Namen des Schlüssels in der iSeries-Datei

➢ KDNR
- dies ist der Schlüsselfeldname aus Notes, mit dem ein vergleichbarer Eintrag in der iSeries Datei gesucht wird

➢ Distinct
- mit dieser optionalen Angabe werden doppelte Werte aus einer Liste gelöscht

Das Ergebnis kann dann nach Eingabe der Kundennr. „A“ wie folgt aussehen:



Ergebnis

Bei der Verwendung von @DBLookup ist darauf zu achten, dass diese Funktion max. 64KB pro Ausführung übertragen kann.

11.3.3.2 @DBColumn

Neben der Funktion @DBLookup bietet @DBColumn eine weitere Möglichkeit, um auf externe Daten zuzugreifen.

Wie auch @DBLookup, so setzt @DBColumn auf einer ODBC-Verbindung auf und nutzt den ODBC-Treiber für den gezielten Zugriff auf die externen Daten. Im Unterschied zu @DBLookup wird nicht ein einzelner Wert einer Spalte zurückgegeben, sondern alle in dieser Spalte (oder dem Feld) enthaltenen Informationen.

Dies wäre – aus Sicht eines iSeries-Entwicklers – vergleichbar mit einem

➢ SETLL
➢ DOUEQ
➢ READE
ENDDO

Aus SQL-Sicht würde dieser Befehl einem

„SELECT …FROM“

entsprechen

Mit @DBColumn können nur Lesezugriffe durchgeführt werden. Datenmanipulationen an den externen Daten sind somit nicht möglich!

Das nachfolgende Beispiel soll das verdeutlichen:

Wir greifen dabei auf dieselben Informationen zu wie im Beispiel zu „@DBLookup”. Dabei listen wir alle Kunden auf, die sich in der Datei „KUNDPF1“ befinden.

Kundenliste

Das Feld „KListe“ haben wir als „berechnetes Feld“ definiert. Dabei ermitteln wir dessen Werte wie folgt:

DBColumn

Die Angaben sind durchaus vergleichbar mit denen der Anweisung @DBLookup – es entfallen jedoch die Angaben der Schlüsselfelder.

Mit dieser Anweisung geben wir in dem Beispiel an:

➢ Zugriff auf eine externe Datenquelle
- „ODBC“

➢ ODBC-Verbindungsname
- „S6524C3C“

➢ Keine Angabe eines Benutzers / Kennworts
- „";„"; Angabe

➢ Pfad und Name der Zieldatei
- Angabe „DOMIS.KUNDPF1“, wobei „DOMIS“ die Bibliothek und „KUNDPF1“ die Datei auf der iSeries ist

➢ Angabe des Feldnamens, dessen Inhalte übertragen werden sollen
- „KUNAME“ –> Dies ist der Feldname aus der iSeries-Datei, dessen Inhalte in das Notes-Feld übertragen werden sollen.

Das Ergebnis dieser Anweisung kann dann wie folgt aussehen:

Ergebnis

Wie Sie sehen, werden alle Einträge, die sich in der Zieldatei „KUNDPF1“ in dem Feld „KUNAME“ befinden, mit dieser einen Anweisung als Liste an Notes übetragen. Dabei werden die einzelnen Werte jeweils durch einen Separator in Form eines „;" getrennt.

11.3.3.3 @DBCommand

@DBCommand stellt mit die leistungsstärkste Anweisung im Zusammenhang mit dem Zugriff auf externe Daten bereit – denn neben den reinen Lesezugriffen der beiden anderen @DB-Befehle kann mit der Verwendung jede SQL-Anweisung übergeben werden – somit ist bei der Verwendung des Befehls @DBCommand auch das Manipulieren der externen Daten möglich.

Die Syntax des Befehls ist wieder vergleichbar mit der der beiden anderen @DB-Befehle.

Schauen wir uns wieder ein Beispiel an, das die Verwendung von @DBCommand zeigt:

Wir haben wieder eine Maske in Notes mit einem Feld, in das wir eine Auflistung der Kunden setzen wollen.

Maske für DBCommand

Das Feld „KListe“ ist ein berechnetes Feld, in das eine Liste der Kundennamen importiert werden soll.

SELECT-Anweisung

Mit diesem Befehlsstring greifen wir auf die externen Daten zu und ermitteln alle Kundennamen aus der Datei „KUNDPF1“ in der Bibliothekl „DOMIS“.

Wie Sie sehen, sind die übrigen Parameter in ihrer Verwendung gleich den Befehlen @DBLookup und @DBColumn – deshalb möchte ich diese nicht nochmals näher erläutern.

Wir benötigen also für die Ausführung dieses Befehls einen ODBC-Zugriff auf eine externe Datei und können dann mit entsprechenden SQL-Angaben auf diese Daten zugreifen und sie bei Bedarf auch manipulieren.

Doch schauen wir uns zunächst noch das Ergebnis der oben gezeigten Anweisung an:

Ergebnis

Erstellen wir eine Aktion, mit der wir alle Datensätze ändern. Wir fügen nun mit einer „UPDATE"-Anweisung in das Feld „KUVERT" ein. Dabei werden alle Datensätze verarbeitet, deren Feldinhalt „KUVERT" leer ist.

Update

Dies soll nur ein Beispiel für eine Datenmanipulation sein. Auf diese Art und Weise können alle SQL-Anweisungen von Notes auf eine iSeries-Datei abgesetzt werden.

Diese Seite ist zur Zeit nicht belegt.

12

Der Domino Webserver

August 2003 / 14. EL

Neben dem Einsatz als E-Mail, Datenbank- und Applikationsserver hat Lotus seit der Version 4.x den Lotus Domino Server mit einem HTTP-Stack ausgestattet. Dieser ermöglicht es, einen Lotus Domino Server als Webserver einzusetzen.

Der Lotus Domino Server besitzt im Verhältnis zu anderen Serverlösungen eine Reihe von zusätzlichen Funktionen:

- bestehende Lotus Notes-Datenbanken können dynamisch in HTTP-Quellcode umgesetzt werden,

- das vorhandene Sicherheits- und Zugriffskonzept des Lotus Domino Servers kann genutzt werden,

- auf einem Server können mehrere virtuelle Domino Server parallel betrieben werden.

Besonders hervorzuheben sind dabei vor allem die dynamischen Funktionen der Lotus Domino-Programmierumgebung. Sie bieten die Möglichkeit, Inhalte flexibel zu gestalten und sind trotzdem in der Wartung überschaubar, weil kein zusätzliches Datenbanksystem notwendig ist. Diese Funktionen sind im Domino Server bereits enthalten. Eine Domino Website kann aus einer Datenbank oder aus mehreren Datenbanken bestehen, die durch Links verbunden sind. Ab Release 5 bietet der Domino Server auch „Passthru-HTML", also die Möglichkeit, HTML in einer Notes-Datenbank zu speichern und direkt an den Browser weiterzugeben. Während eine konventionelle Verwaltung von Webseiten zu einer weit verzweigten Dateiorganisation führt, können die Daten und Programme beim Domino Server in wenigen Datenbanken gespeichert werden.

Die Einrichtung eines Domino Servers als Webserver gliedert sich in zwei Bereiche: die Konfiguration des Servers und die Erstellung der eigentlichen Website. Die Seiten können in einer Lotus Notes-Datenbank oder als HTML-Dokumente im herkömmlichen Stil gespeichert werden.

12.1 Einrichten eines Domino Servers als Webserver

Das Einrichten des Domino Servers gliedert sich in die folgenden Schritte:

1. **Der Domino Server**
   Die Grundlage des Webservers bildet der Lotus Domino Server. Um den Server über das Internet oder Intranet für die Benutzer verfügbar zu machen, muss das Netzwerkprotokoll TCP/IP aktiviert sein.

Um es zu aktivieren oder zu prüfen, ob TCP/IP aktiviert ist, gehen Sie wie folgt vor:

❶❷❸ Ausführungsschritte:

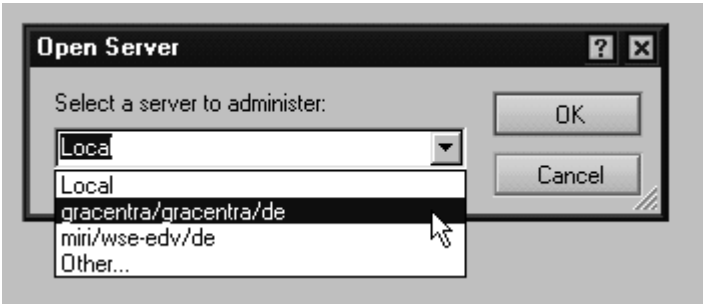
1. Starten Sie den Client.

2. Wechseln Sie in das Server-Dokument des Servers, auf dem die Website eingerichtet werden soll.

3. Wählen Sie die Domäne aus.

Domäne wählen

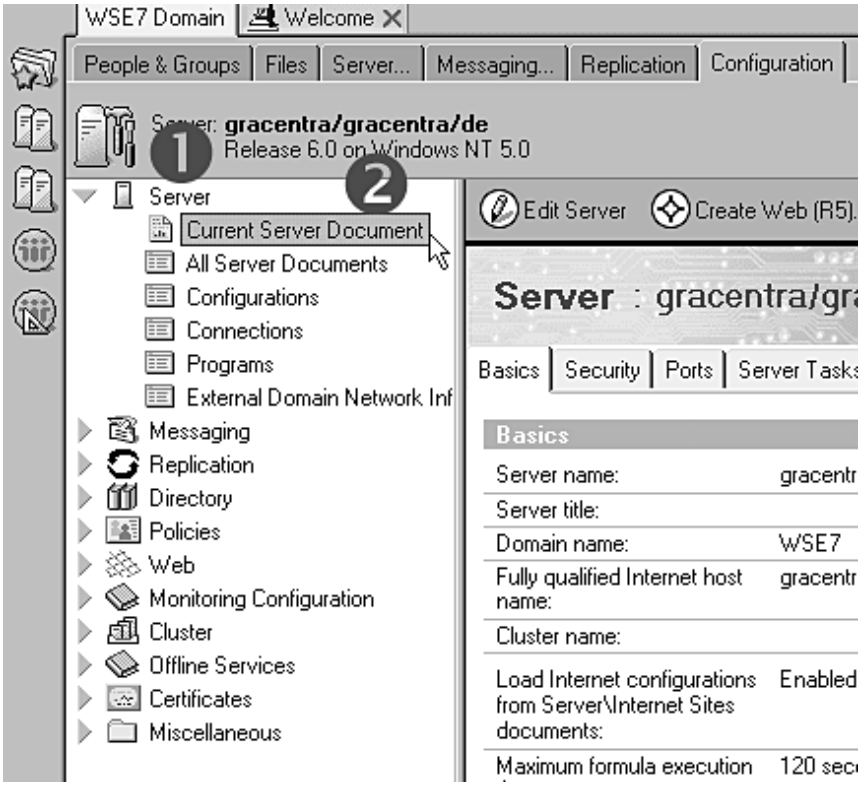
4. Wählen Sie über das Menü „File“ – „Open Server“ dort in der Auswahlbox den gewünschten Server aus.



Open Server

5. Nun klicken Sie im linken Übersichtsfenster doppelt auf den Server ❶,

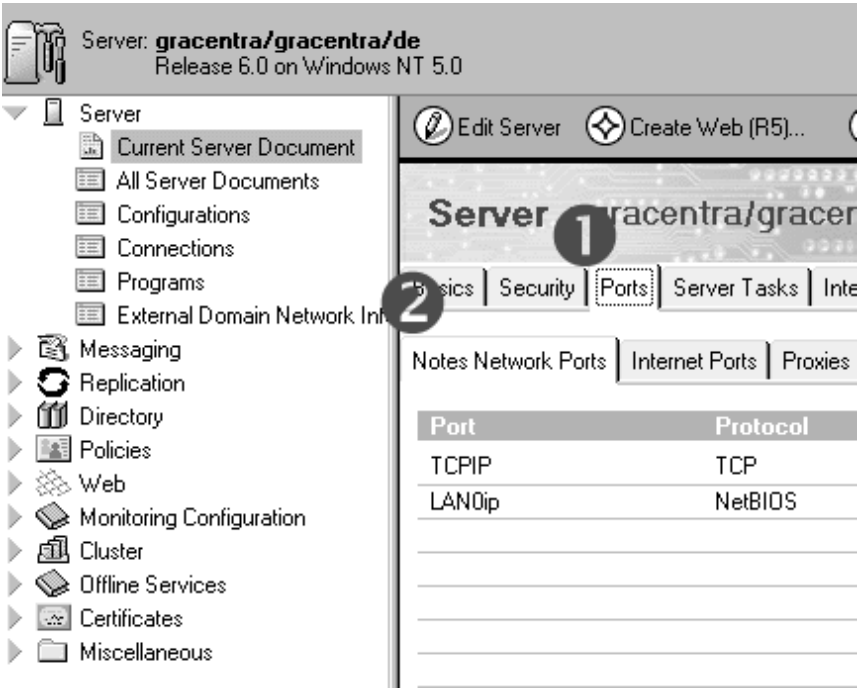
6. Anschließend klicken Sie nochmals doppelt auf „Current Server Document“ ❷.



Serverdokument wählen

Damit ist das Konfigurationsdokument des Servers ausgewählt.

Im Konfigurationsdokument wird im Bereich Ports ❶ und da unter dem Register „Notes Network Ports“ ❷ eingestellt, welche Netzwerkprotokolle aktiviert sein sollen.

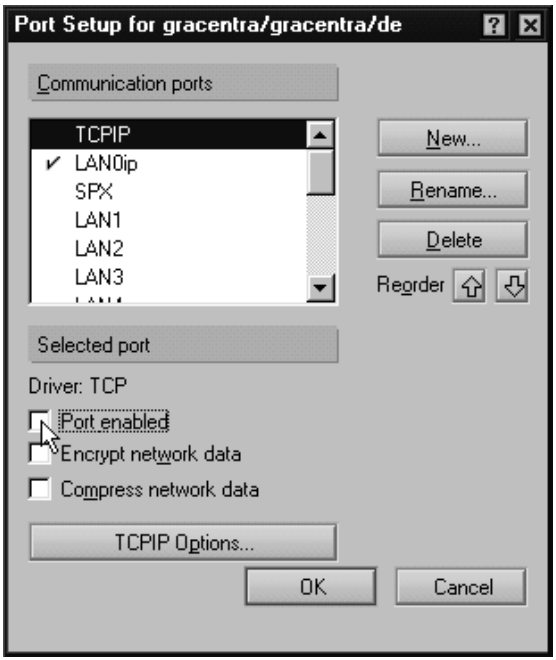


Netzwerk

Die Aktivierung des TCP/IP-Protokolls erfolgt, indem im Menü „Werkzeuge“ auf der rechten Seite des Dokuments unter „Server“ der Punkt „Setup Ports“ ausgewählt wird.

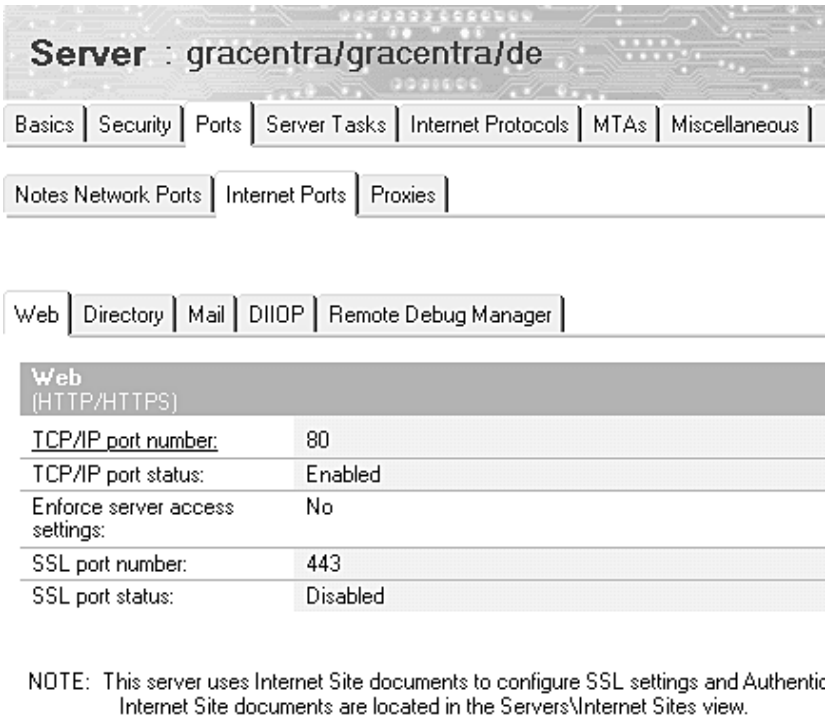
Netzwerk-Protokoll aktivieren

Über diese Menüposition wird ein Dialogfenster gestartet. Hier werden alle verfügbaren Netzwerkprotokolle angezeigt. Durch Anhaken aktivieren Sie das TCP/IP-Protokoll.



TCP/IP-Port aktivieren

Auch die Ports, über die die HTTP-Pakete geschickt werden sollen, müssen aktiviert sein. Hierfür wird das Register mit der Bezeichnung „Internet Ports“ rechts neben dem Reiter „Notes Network Ports“ verwendet.



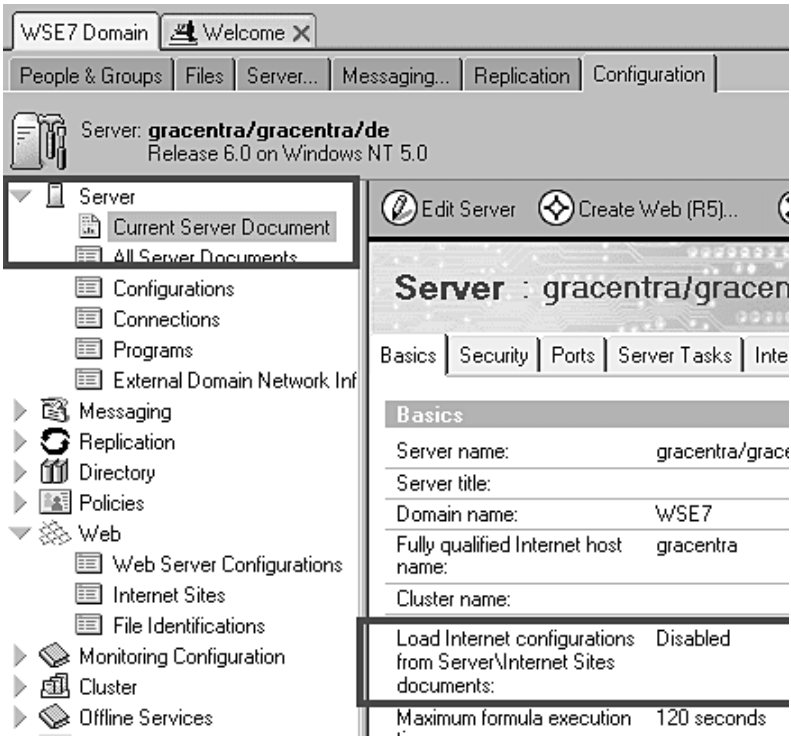
Ports konfigurieren

Hier sind die Standardports für HTTP (Port 80) und SSL (Port 443) eingetragen. Eine detailliertere Beschreibung finden Sie weiter hinten im Kapitel „Anpassen der TCP/IP-Standardeinstellungen (Ports und Protokolle)."

2. **Strategie für Internetverbindungen**
   Falls der Zugriff über das Internet möglich sein soll, muss der Lotus Domino Server mit einem Internet Service Provider (ISP) verbunden werden, seine gewünschte Web-Adresse und die IP-Adresse müssen auf dem DNS-Server des Internet Providers eingetragen werden. Falls Sie hier Unterstützung benötigen, ist der Administrator des Internet Providers der richtige Ansprechpartner.

3. **Nun kann der Lotus Domino Server gestartet werden.**

4. **Serverdokument des gewünschten Servers öffnen.**
   In der Ansicht des Registers „Allgemein" wird im Feld „Load Internet configurations from Server\Internet Sites documents" aktiviert, dass die Konfigurationsparameter der Website aus den Dokumenten der Webseitenansicht geladen werden sollen.



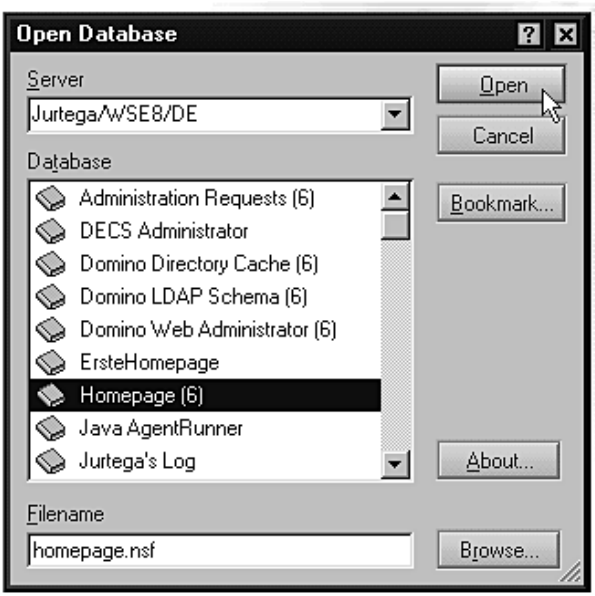
Konfiguration aus der Webseitenansicht laden

5. **Für den Betrieb des Webservers ist es notwendig, mindestens ein Webseitendokument zu erstellen.**
   In dem Webseitendokument werden die notwendigen Parameter für den Webserver eingestellt und verwaltet.

6. **Zum Aktivieren wird der HTTP-Task gestartet.**
   Um die Einstellungen zu testen, wird ein Internet-Browser gestartet. In der URL-Zeile wird die Web-Adresse oder die IP-Adresse eingegeben, die konfiguriert wurde.

12.2 Basisdatenbank für eine Website erstellen

Prinzipiell kann der Lotus Domino Webserver jede beliebige Lotus Notes-Datenbank als Website darstellen. Ein Beispiel für eine Datenbank, die speziell für das Internet angepasst ist, ist die Datenbank „homepage.nsf“, die im „data“-Verzeichnis des Lotus Domino Servers bei der Installation angelegt wird.

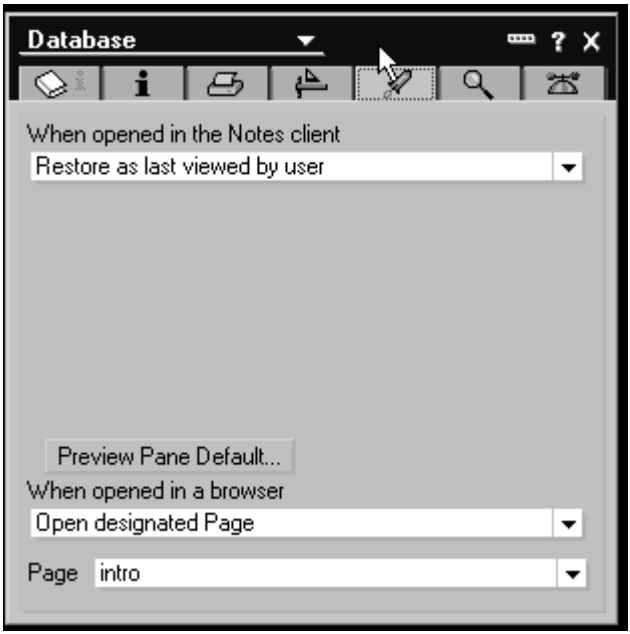


Beispieldatenbank „homepage.nsf“

Wenn diese Datenbank mit dem Lotus Notes Designer geöffnet wird, kann man erkennen, dass in diesem einfachen Beispiel nur eine Seite angelegt wurde, auf der ein Bild als Hintergrund dient

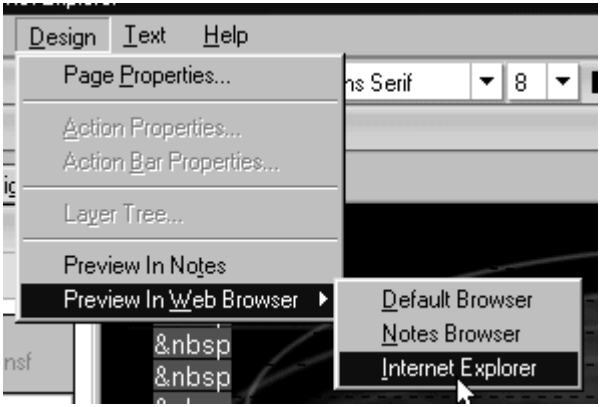
August 2003 / 14. EL

und bei dem mithilfe einer Tabelle mehrere Möglichkeiten zur weiteren Verzweigung angeboten werden. Die Seite, die in einer Notes-Datenbank als erstes geöffnet werden soll, wird über die Eigenschaften der Datenbank (Menü „Datei / Datenbank / Eigenschaften“) im Feld „When opened in a browser“ festgelegt.



Festlegung der Startseite

Dann wird im Abschnitt „Seite“ über die Schaltfläche „Neue Seite“ eine neue Seite erzeugt. Diese Seite kann wie ein normales Formular von Lotus Notes erstellt und gespeichert werden. Über den Menüpunkt „Gestaltung / Vorschau im Webbrowser / Internet Explorer“ können Sie die neu erstellte Seite testen.



Testen

Wenn diese Datenbank verwendet werden soll, ist in den oben angeführten Feldern entsprechend der Name „/data/homepage.nsf“ einzutragen.

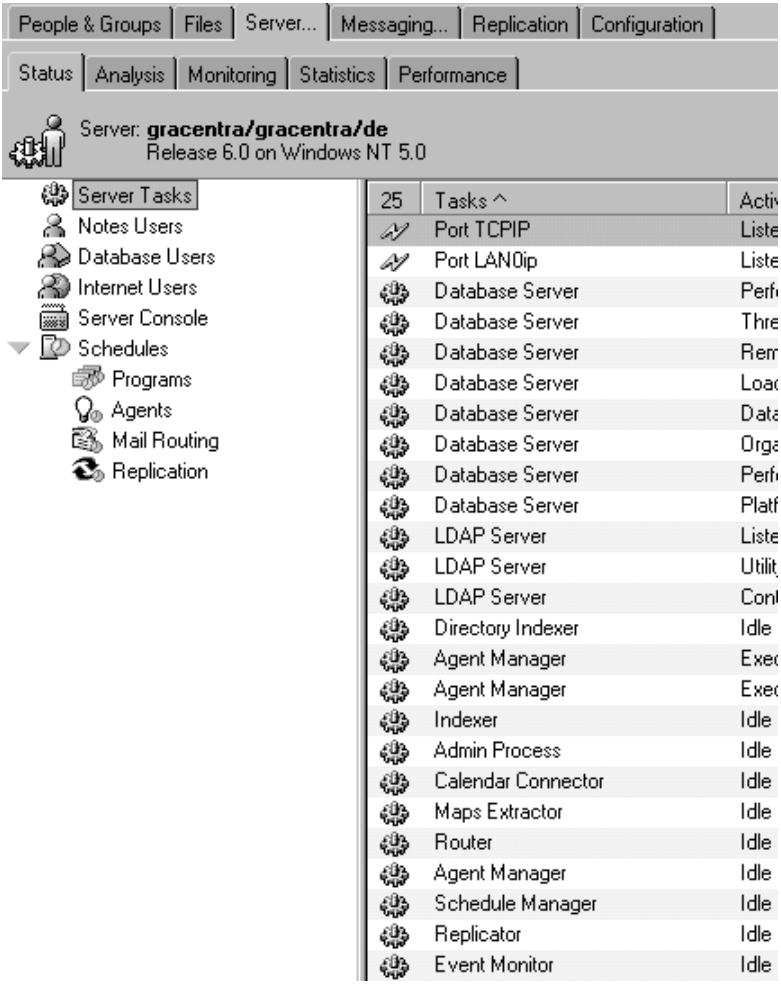
Diese Seite ist zur Zeit nicht belegt.

12.3 Referenzteil zum Domino Webserver

Der folgende Abschnitt bietet die Möglichkeit, über die notwendigen Standardeinstellungen hinweg Informationen zu Konfiguration und Administration des Lotus Domino Webservers nachzulesen.

1. **Starten und Stoppen des Domino Webservers**
   Der HTTP-Task wird bei einer normalen Installation bereits mitinstalliert. Vor dem Starten des HTTP-Tasks sollte auf jeden Fall eine Webseite erstellt und konfiguriert werden. Anschließend kann der Task mit dem Befehl „load http“ an der Domino-Konsole gestartet werden. Beendet wird entsprechend mit dem Befehl „tell http exit“. Als Alternative kann das Starten und Beenden auch über den Lotus Administrator-Client laufen.

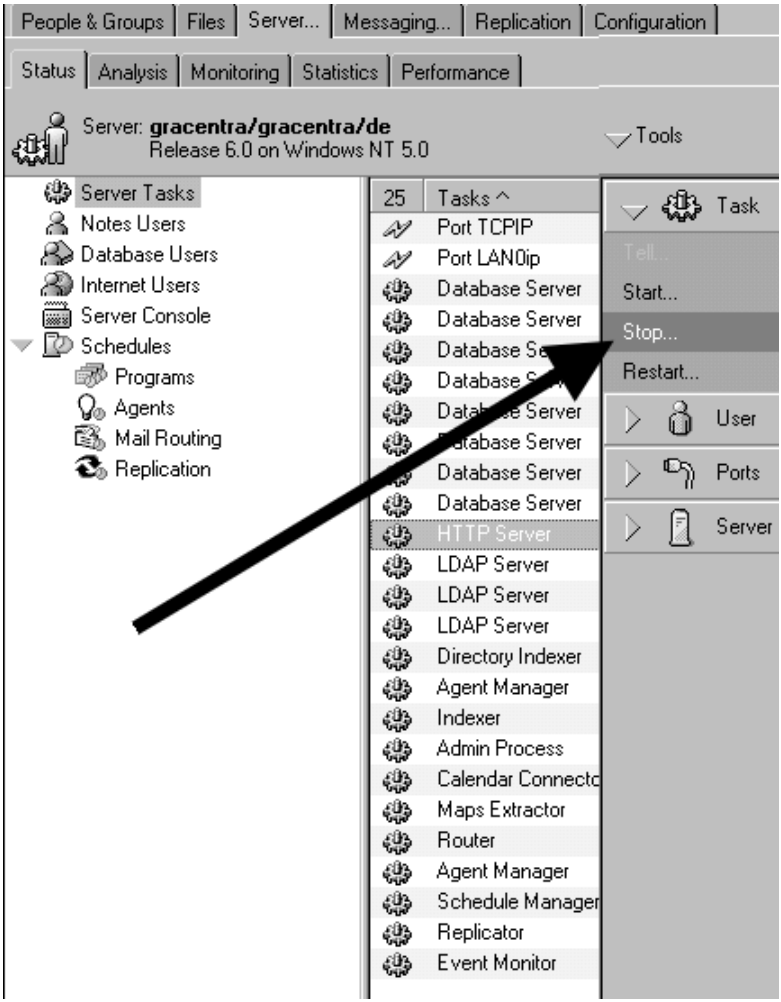
August 2003 / 14. EL



Liste der HTTP-Tasks

Hierzu wird zunächst der Server, auf dem der Task gestartet werden soll, ausgewählt. Hinter dem Reiter „Server“ befindet sich der Reiter „Status“. Nachdem der aktuelle Status der Tasks vom Ser-

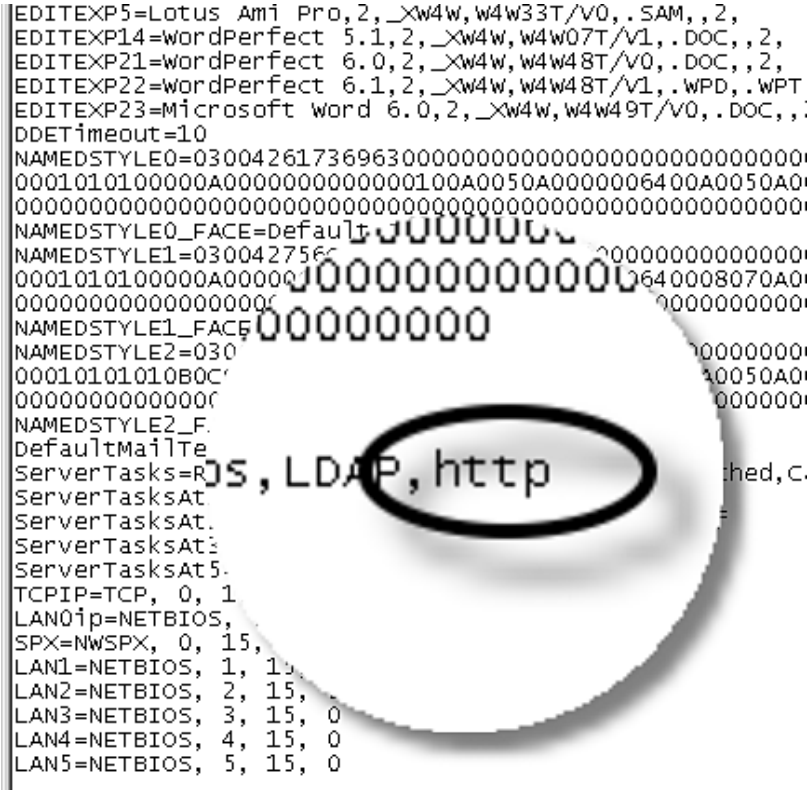
ver geladen wurde, kann über die Auswahl „Start“ rechts in der Toolbar ein Task ausgewählt werden, der gestartet werden soll.



HTTP-Task stoppen

Der zu startende Task ist unter der Bezeichnung „HTTP Web Server“ zu finden. Zum Beenden des Tasks klicken Sie mit der Maus einmal auf den gestarteten Task und wählen dann in der Toolbar rechts „Stop Task“ aus. Nun wird der Task beendet.

Nach der Eingabe oder einer Veränderung von Einstellungen ist es notwendig, den Server zu stoppen und wieder neu zu starten. An der Befehlskonsole des Domino Servers kann dazu der Befehl „tell http restart“ eingegeben werden.



HTTP-Task automatisch starten

Damit der HTTP–Task automatisch beim Starten des Servers aktiviert wird, ist ein Eintrag in der Datei notes.ini in der Zeile „Servertasks“ im Programmverzeichnis des Lotus Domino Servers notwendig (z.B. „C:\Lotus\Domino\notes.ini“, wenn der Standardvorschlag des Setup-Programms übernommen wurde).

2. Anpassen der TCP/IP-Standardeinstellungen (Ports und Protokolle)

Mit den Einstellungen, die bei der Installation des Lotus Domino Servers im Serverdokument vorgenommen werden, kann man den Webserver ohne Änderungen betreiben. Im Folgenden wird kurz erläutert, welche Bedeutung die einzelnen Felder haben:

TCP/IP – port number

Die Portnummer des HTTP-Ports kann in dem Feld „TCP/IP port number“ geändert werden, wenn sich diese z.B. durch die Verwendung einer Firewall geändert hat.

TCP/IP port status

In dem Feld „TCP/IP port status“ kann der Port komplett deaktiviert werden, wenn ein Zugriff verhindert werden oder z.B. nur der SSL-Port verwendet werden soll. Dann wird hier „redirected“ aktiviert, um alle Pakete auf den SSL-Port umzuleiten.

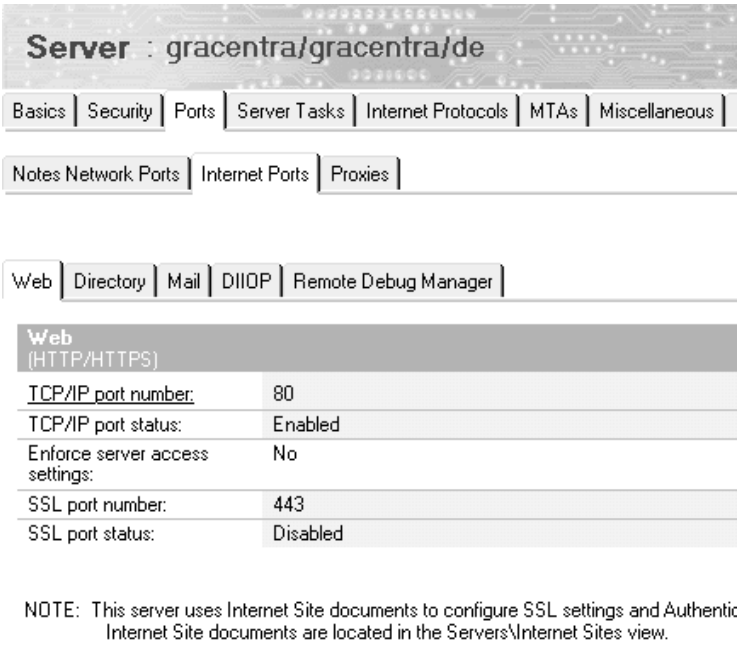
Enforce server access settings

Wenn im Feld „Enforce server access settings“ die Auswahl „yes“ getroffen wird, werden die Einstellungen bezüglich des Benutzerzugriffs aus dem Security-Reiter des Serverdokuments erzwun-

gen. Dort kann der Zugriff für bestimmte namentlich aufgeführte Benutzer gewährt oder auch verweigert werden.

SSL port number
Der Port, der für den SSL-Zugriff verwendet werden soll, wird hier festgelegt. Standardmäßig ist hier der richtige Port 443 durch die Installation vorbelegt.

SSL port status
Der SSL-Port des Lotus Webservers kann hier aktiviert oder deaktiviert werden.



Ports konfigurieren

3. **Einrichten von Sicherheitsparametern für Internetprotokolle**
   Zusätzlich zu den bisher beschriebenen Möglichkeiten bietet der HTTP-Server eine Reihe von weiteren Einstellungen, die Angriffe auf den Webserver verhindern sollen: Blockade von Buffer-Overflow-Attacken oder die Erzeugung von Abfragefehlern.

Die Einstellungen für die Protokollsicherheit befinden sich unter dem Reiter „Internet Protocols“ und dort im Bereich des Reiters „HTTP“.

HTTP Protocol Limits	
Maximum URL length:	4 kilobytes
Maximum number of URL path segments:	64
Maximum number of request headers:	48
Maximum size of request headers:	16 kilobytes
Maximum size of request content:	10000 kilobytes (specify 0 to allow unlimited content)

HTTP-Protokollbeschränkungen

Hier muss ganz nach unten geblättert werden, wo auf der rechten Seite dann die folgenden Felder bearbeitet werden können:

Maximum URL length
Eine Art der Angriffe auf Webserver besteht darin, sie mit URLs zu beschicken, die so lang sind, dass sie einen Speicherüberlauf beim Laden bzw. Verarbeiten durch den Server verursachen. Um

hier Schutz zu bieten, wurde die Möglichkeit geschaffen, die Länge einer URL, die der Lotus Domino Webserver akzeptiert, zu begrenzen. Als Voreinstellung wird von Lotus 4 KB eingestellt, was für fast alle Anwendungen völlig ausreichend ist.

Maximum number of URL path segments
Als ein Pfadsegment werden die Zeichen zwischen zwei Schrägstrichen „/“ bezeichnet. Die voreingestellten 64 Segmente als Obergrenze werden nur in wenigen Fällen überschritten werden.

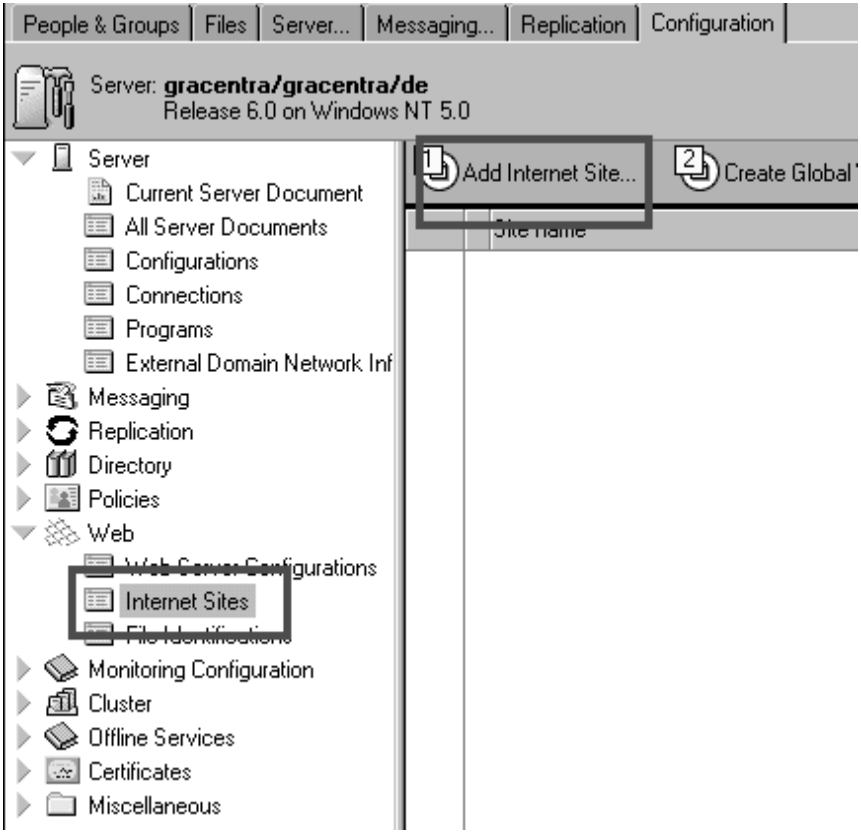
Maximum number of request headers
Hier wird die maximale Anzahl an HTTP-Anfrageköpfen festgelegt. Die Voreinstellung ist 48. Diese Zahl muss normalerweise nicht erhöht werden, da die Anfragen eines Webbrowsers gewöhnlich weniger als ein Dutzend Köpfe enthalten.

Maximum size of request content
In diesem Feld wird die maximale Datenmenge festgelegt, die ein Benutzer vom Lotus Domino Server über den HTTP-Task anfordern oder die er an den Server schicken kann. Wenn keine Daten an den Server geschickt oder vom Server geholt werden sollen, kann die Grenze weit unter den 10 MB liegen, die als Vorgabewert eingestellt sind.

4. Erstellen eines Webseitendokuments für Lotus Domino
Die folgenden Schritte müssen ausgeführt werden, um ein Webseitendokument zu erstellen:

❶❷❸ Ausführungsschritte:

1. **Im Domino Administrator Client wird „Konfiguration / Web / Internet-Seiten“ ausgewählt.**



Web-Seiten definieren

2. **Durch Klicken auf die Schaltfläche „Add Internet Site“ wird ein Dokument für die Internet Site angelegt.**

3. **Einstellungen Register „Allgemein“**
   Unter dem Register Allgemein” müssen die folgenden Felder ausgefüllt werden:

Beschreibender Name der Seite (optional)
Der Name der Seite sollte so gewählt werden, dass sie von anderen Seiten, die hier angelegt werden, unterschieden werden kann.

Organisation (zwingend erforderlich)
Hier wird der Name der Organisation eingegeben, bei der das Webseiten-Dokument gehostet wird.

„Use this Web site to handle requests which cannot be mapped to any other Web sites“
Hier kann ausgewählt werden, ob diese Seite als Standardseite für Requests benutzt werden soll, die auf eine andere Seite verweisen. Wenn hier „Ja“ gewählt wird, dann werden HTTP-Requests, für die Domino keine Webseite finden kann, trotzdem verarbeitet. Wenn Sie „Nein“ wählen, so werden Anfragen, die nicht verarbeitet werden können, abgewiesen.

„Host names or adresses mapped to this site“ (erforderlich)
Hier wird der Name oder die IP-Adresse eingetragen, die die Benutzung der Verbindung zu diesem Internet Site-Dokument auslöst. Wenn bei dieser Site mit SSL gearbeitet werden soll, muss eine IP-Adresse verwendet werden.

„Domino Server that host this site“
Alle Domino Server, auf denen die Webseiten der Internet-Site verteilt sind, werden hier mit ihrem Namen eingetragen. Dabei kann jede Art Name und können auch Wildcards verwendet werden.

Der Standardwert in diesem Feld ist „*“, also alle Server in der Domäne können die Internet Site hosten.

Wenn dieses Feld leer bleibt, wird die Site auf keinem Domino Server gespeichert.

4. Das Register „Konfiguration“
In diesem Bereich werden vor allem Einstellungen zu der Homepage und den Einstellungen der verschiedenen Pfade vorgenommen.

„Home URL“
Hier wird die URL eingetragen, die dem Benutzer angezeigt werden soll, wenn er nichts außer der Webadresse als URL eingegeben hat. Wenn also nur „www.wse-edv.de“ eingegeben wurde, dann wird in der Regel auf einen anderen Link, wie z.B. „/welcome.nsf/hello?OpenPage“ verwiesen.

„HTML-Verzeichnis“
Hier wird das Verzeichnis angegeben, in dem sich HTML-Seiten befinden, wenn nicht explizit die komplette URL im HTML-

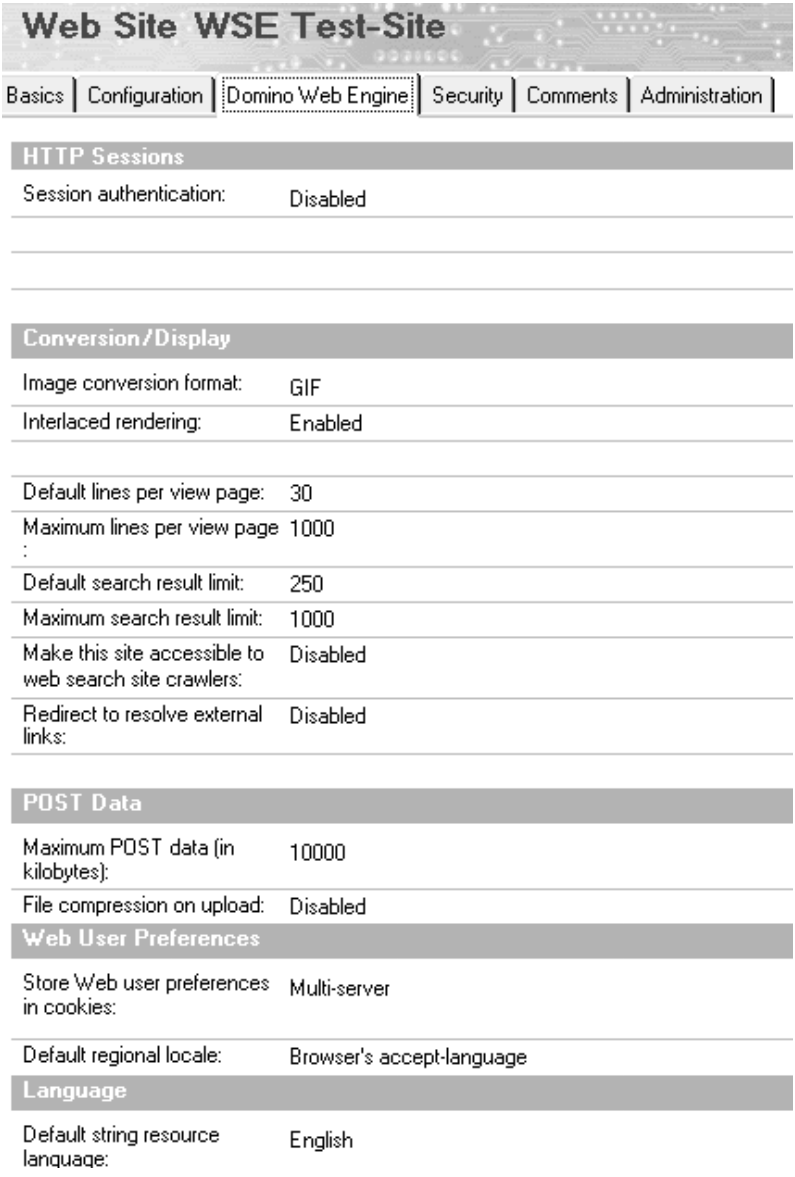
Quelltext gespeichert wurde. Es besteht dann die Möglichkeit, statt „http://www.wse-edv.de/welcome.html“ nur „welcome.html“ anzugeben. Die Vorgabe für dieses Feld ist „domino\html“. Der Pfad kann relativ zum Domino-Data-Verzeichnis angegeben werden: etwa als „domino\meinHtml“ oder es kann der komplette Pfad eingepflegt werden. „C:\websites\wse-edv.de\html“ wäre hierfür ein Beispiel.

Der Lotus Domino Server sucht in gesondert aufgeführten Verzeichnissen nach individuellen HTML-, CGI- und Icondateien auf der Festplatte des Servers. Bei CGI-Programmen und Icon-Dateien kann eine URL angegeben werden.

Die Verwendung dieser Pfade und Verzeichnisse ist besonders dann sinnvoll, wenn sich der Ort ändert, an dem sich die CGI-Programme und die Icon-Dateien befinden. Sie werden nach einer Änderung und einer Anpassung des Pfades ohne Modifikation des HTML-Quelltextes sofort wieder gefunden.

5. Domino Web-Engine

Das Register für die „Domino Web-Engine“ bietet die Möglichkeit, eine Reihe von Parametern mit Werten zu versehen, die für die Übertragung und Sitzungsinformationen verwendet werden.



Domino Web-Engine konfigurieren

Felder

Einstellen der „Session Authentication“
Für ein Webseitendokument kann ausgewählt werden, dass der Zugriff nur über einen Login mit entsprechender Sitzungsidentifizierung erlaubt ist. Für den Zugriff muss dann ein Browser verwendet werden, der Cookies unterstützt. Hiermit kann ein HTML-Login eingerichtet werden, über den Benutzer sich identifizieren müssen und bei dem sich die Benutzer auch wieder abmelden können. Diese Sitzungen können bei Bedarf protokolliert werden.

Art der Umwandlung von GIF- und JPEG-Dateien
Die Art, wie die Bilder der Web-Seite angezeigt werden, kann hier eingestellt werden. Diese Einstellungen gelten nur für GIF- und JPG-Dateien und nicht für Passthrough-HTML. Wenn entweder progressives Rendering oder interlaced Rendering ausgewählt wird, dann scheint das Bild schneller geladen zu werden und es kann normalerweise schon erkannt werden, bevor es ganz heruntergeladen wurde.

Anzuzeigende Zeilen in einer Ansicht
Über diese Einstellung kann die Anzahl der Zeilen, die in einer Ansicht angezeigt werden sollen, begrenzt werden. Besonders bei großen Datenbanken kann es die Übersicht verbessern, wenn hier eine entsprechende Einschränkung vorgenommen wurde.

Anzahl Dokumente begrenzen, die bei einer Suche angezeigt werden sollen
Ebenso können Sie die Anzahl der Dokumente, die als Ergebnis einer Suche angezeigt werden, auf eine bestimmte Anzahl an Zeilen begrenzen. Diese Einstellung dient dazu, zu verhindern, dass der Lotus Domino Server mit Suchanfragen überlastet werden kann.

Links mit dem „Redirect URL“-Befehl finden
Wenn auf einer Webseite Links auf Dokumente, Ansichten oder Datenbanken angelegt werden sollen, dann erfolgt dies über den „Redirect URL“-Befehl. Solche Links und Links, die aus einer Domänensuche entstehen, können Benutzer dann auf eine Datenbank auf dem gleichen oder einem anderen Lotus Domino Server umleiten. Die Option muss auf jedem Server, der in die Domänensuche eingeschlossen werden soll, sowie auf allen Servern, auf die weitergeleitet werden können soll, eingerichtet werden.

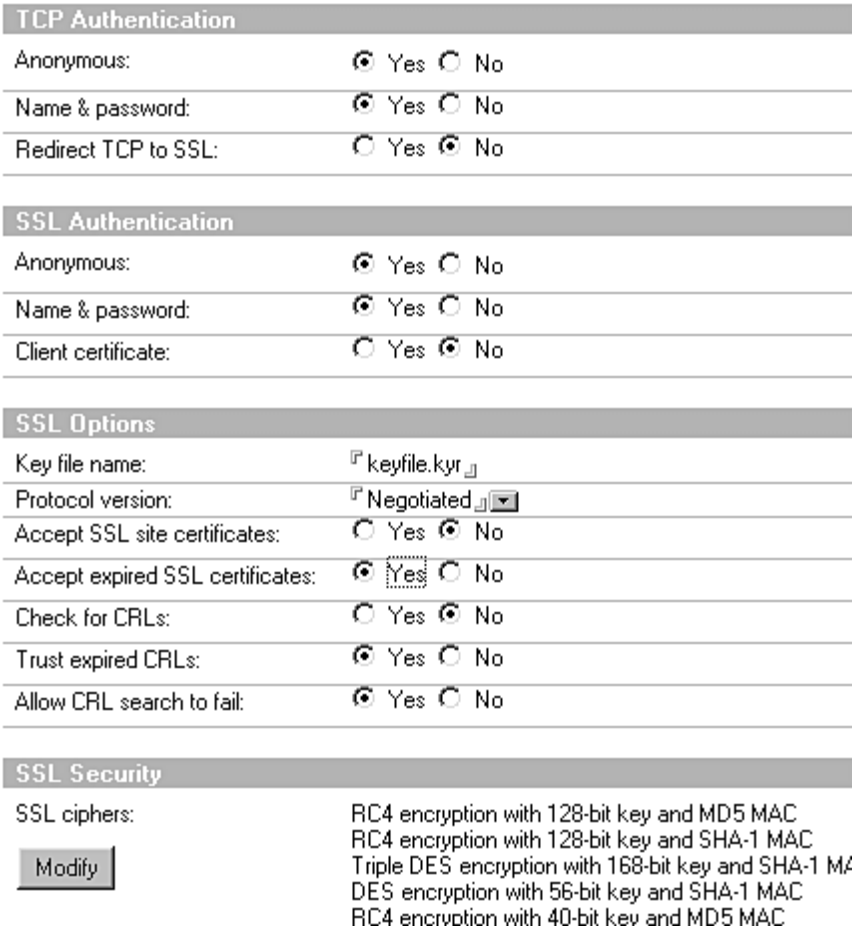
Beschränken der Datenmenge, die ein Benutzer an eine Domino-Datenbank senden kann.
Um das Überladen eines Lotus Domino Servers mit zu großen Datenmengen zu verhindern, wurde in der Version 6 ein Limit für die beiden HTTP-Methoden POST und PUT eingeführt. Die Maximalgrenze gilt für alle POST- und PUT-Methoden, ganz gleich ob das Ziel eine Datenbank, ein CGI-Programm oder ein Java-Servlet ist und sie gilt für alle Websites.

Preferenzen von Webbenutzern in Cookies speichern
Wenn es gewünscht wird, dass Web-Benutzer Ihre Zeitzone und ihre regionalen Voreinstellungen speichern können, muss diese Option aktiviert werden. Dabei ist zu beachten, dass der Benutzer einen Web Client benutzt, der dies zulässt.

Festlegen eines internationalen Zeichensatzes beim Bereitstellen einer Seite
Hier kann die Standardsprache für Zeichenketten angegeben werden, die der Server an den Browser schickt.

6. Das Register „Sicherheit“

Unter dem Sicherheitsregister finden sich hauptsächlich die Einstellungen für Verbindungen, die mit der Secure Socket Layer (SSL) -Verschlüsselung aufgebaut werden sollen



Das Register Sicherheit

TCP Authentication
Zunächst wird eingestellt, ob es möglich sein soll, einen anonymen Zugang zu der Webseite zu erhalten. Falls gewünscht, kann der Zugang dann über Benutzername und Kennwort erfolgen. Um die Sicherheit zu erhöhen, besteht die Möglichkeit, die Verbindung von TCP auf SSL umzustellen und so die übertragenen Daten zu verschlüsseln.

In den folgenden Bereichen werden die verschiedenen Parameter für die SSL-Verschlüsselung eingetragen.

Damit ist die Konfiguration der Parameter für die erste Website abgeschlossen. Die eigentliche Website kann nun in die Lotus Notes-Datenbank, die beim Register „Konfiguration“ eingetragen wurde, eingepflegt werden.